NORTH EASTERN
ICT Partnership

# Local Civic Cyber Resilience

## An Aid to Local Strategy Development

for resilience, business continuity and information security colleagues

**version 1.1**

**North Eastern ICT Partnership**

Councils working together on IT:

Northumberland~Newcastle~North Tyneside
Gateshead~South Tyneside~Sunderland~Durham
Stockton~Darlington~Nexus

**Spring 2018**

## Foreword

Cyber Security is a Tier One National Security risk, alongside pandemic, terrorism and environmental risks. The potential business impacts of a cyber-attack are disruption of services, threat to service users' (customers') safety, reputational damage and the demand for post-event/breach resources required to demonstrate compliance. Focussing on the resilience of local public services in the event of a of a cyber-attack should help us gain discussion time at board-level.

One element of meeting the demands of a growing cyber security threat to public services is to bring our operations, information management, and civil resilience / contingency communities together; firstly, within our organisations and then, because of the increased interdependencies and complex relationships between local organisations, at a regional level, probably through Local Resilience Forums and WARPs.

In discussions at NEICT[1] and ISNorthEast[2], colleagues have realised that much of the language used by the resilience and information security communities is alien to the other. There is a need to engage, to exchange knowledge and experience and to plan collaborative responses to the growing cyber threat.

We also recognised, based on experience, that our local resilience plans should consider IT outage scenarios other than cyber-attack (power failure, loss of data centre etc.) as the business impact could be similar.

We've developed this aid to support early-stage discussions between operations, information management, and civil resilience / contingency colleagues. We've tried to keep it simple and focussed on business risk rather than technology. We hope you find it useful.

**Neil Arnold**

Chair of NEICT

Chief Information Officer, Northumberland County Council

[1] North Eastern ICT Partnership – see Appendix 1
[2] Information Security NE – North East Government WARP – see Appendix 2

# Contents

## Background

Since 2015, the Department for Communities and Local Government (DCLG), has been running a programme of engagement with English Local Authorities and their strategic partners on issues relating to cyber resilience. The programme recognised the growing threat of cyber-attacks to all public services and the need for Local Authorities to engage with the wider efforts of the National Cyber Security Programme (NCSP). A significant amount of guidance has been produced (available at Local Civic Cyber Resilience resources).

## An aid to local strategy development

This document aims to break down and augment existing guidance and relate it to the key roles that already exist within many UK Local Authorities.

Key Responsibilities, Recommended Reading and Useful Resources for each key role are suggested, though your organisation may decide these should be distributed differently.

The key roles considered are:

- Councillors
- Chief Executive Officer (CEO)
- Senior Information Risk Owner (SIRO)
- Local Resilience Manager (LRM)
- Business Continuity Manager (BCM)
- Service Managers and Information Asset Owners
- Data Protection Officer (DPO)
- Head of IT (HoIT)
- Information Security Manager (ISM)

This could easily be adapted for use by other organisations such as academic institutions and private companies.

It should be stressed that much of the activity described in the following sections is already being undertaken and that such individuals will have related responsibilities beyond civic cyber resilience.

Your organisation may be structured differently, particularly in the area of business continuity and resilience where these may not be separate roles.

| | |
|---|---|
| • Councillors | Sponsor a local civic cyber resilience programme, provide adequate resources |
| • Chief Executive Officer (CEO) | Ultimately responsible for local civic cyber resilience |

| | |
|---|---|
| • Senior Information Risk Owner (SIRO) | Own and oversee the implementation of the organisation's Cyber Resilience Strategy<br>Chair local cyber resilience group; represent Service Managers and escalate / cascade knowledge to / from these |
| • Local Resilience Manager (LRM) | Support the SIRO with the implementation of the organisation's Cyber Resilience Strategy<br>Lead on regional collaboration and joint working with other public service organisations<br>Ensure resilience plans are tested regularly |
| • Business Continuity Manager (BCM) | Support the SIRO with the implementation of the organisation's Cyber Resilience Strategy<br>Lead on staff training<br>Ensure Service Managers have contingency plans in place covering lack of access to systems/data<br>Ensure resilience plans are tested regularly |
| • Service Managers and Information Asset Owners | Identify measures to minimise the impact of a cyber security incident or computer outage on service delivery and (customer) data |
| • Data Protection Officer (DPO) | Ensure cyber risks to (customer) data are considered |
| • Head of IT (HoIT) | Ensure cyber risks to core corporate IT and Service delivery systems are considered |
| • Information Security Manager (ISM) | Minimise the impact of a cyber security incident or computer outage on systems and (customer) data<br>Manage cyber incident reporting and escalation |

## Validation

This document was circulated for peer review to:

- A number of resilience professionals within Northumbria Local Resilience Forum
- Members of ISNorthEast (NEGWARP), a community of public sector information security professionals from the North East of England
- Contacts within the National Cyber Security Programme – Local, Department for Communities and Local Government

## Contact

Graham Jordan

**Partnership Analyst** and NEGWARP (ISNorthEast) Manager

grahamjordan@gateshead.gov.uk

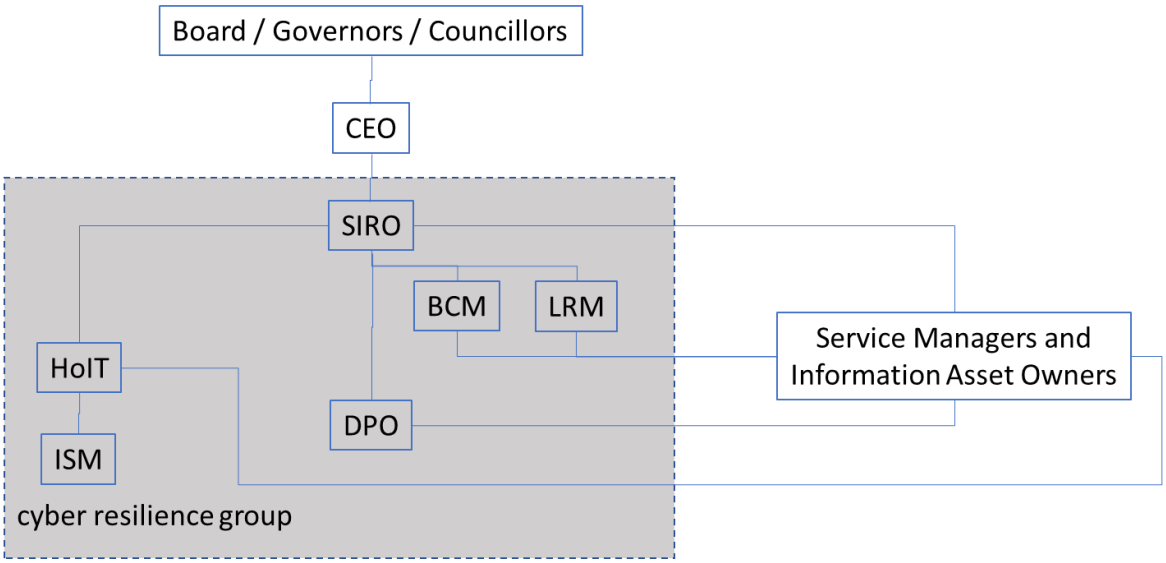
www.neict.org

@neict

tel. 0191 433 3790

## Local cyber resilience group

To aid discussion and strategy development, it is suggested that a local 'cyber resilience group' bringing the key players together is convened:




| | |
|---|---|
| SIRO | Senior Information Risk Owner |
| LRM | Local Resilience Manager |
| BCM | Business Continuity Manager |
| DPO | Data Protection Officer |
| HoIT | Head of IT |
| ISM | Information Security Manager |

## A maturity reference model

You may find it useful to consider your current situation and where you aspire to be; this model may help.

Most organisations will start their local civic cyber resilience journey already being at the 'Aware' level of Maturity. The objective ought to be to move to the 'Embracing' or 'Leading' levels.

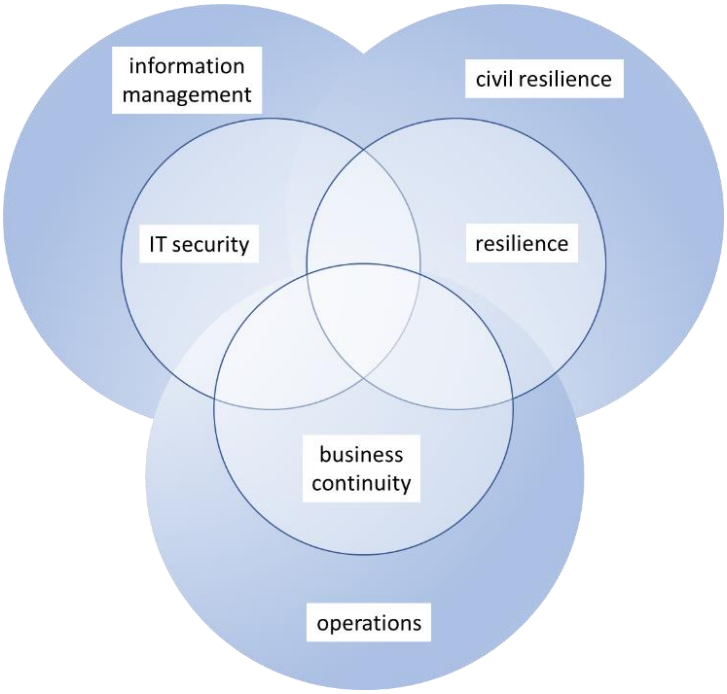
| | | | | |
|---|---|---|---|---|
| *awareness* | *Aware of the "Think Cyber – Think Resilience" programme for local public services* | *Engaged with the "Think Cyber – Think Resilience" programme for local public services* | *Embracing the "Think Cyber – Think Resilience" programme for local public services* | *Taking a lead role in local LRF/WARP activities* |
| *activity* | *Reactive approach* | *Reactive approach* | *Proactive approach* | *Proactive approach* |
| *embeddedness* | *Investigation - briefing documents / management reports* | *Project - Internal Plan in place* | *Programme - Internal Strategy in place* | *Regional strategy in place* |
| *ownership* | *Local Resilience Manager / Head of IT* | *Local Resilience Manager* | *SIRO* | *Regional group* |
| *resources* | *Few dedicated resources* | *Some dedicated resources* | *Multiple dedicated resources* | *Dedicated resources* |
| *measurement* | *No KPIs and KRIs* | *KPIs and KRIs being developed* | *KPI AND KRI-driven, ROI can be calculated* | *Regional KPIs and KRIs in place* |
| **Maturity level** | **Aware** | **Engaged** | **Embracing** | **Leading** |

KPI- key performance indicator KRI - key risk indicator

## Possible roles and suggested responsibilities

These are offered by way of suggestions to aid your local discussions. You may find your organisation would chose to implement these in a different manner.

There are three key communities represented:




- Operations
- Information management
- Civil resilience / contingency

Your organisation may be structured differently, particularly around business continuity and civil resilience. Your organisation may take the view that your SIRO isn't best placed to lead on local civic cyber resilience.

You may wish to add other roles such as a monitoring / assurance role (e.g. Internal Audit, External Audit, External Assessors) in terms of assessment of effectiveness and/or compliance.

Dedicated resources might not be required as they may already exist within ongoing projects.

Your organisation will be best-placed to identify the role of, and requirements for, any collaborative regional strategy.

# Councillors

**Role**

1. Sponsor a local civic cyber resilience programme, provide adequate resources

**Key Responsibilities**

1. Understand the need for Local Civic Cyber Resilience
2. Understand the potential impact of a cyber security incident or computer outage

**Recommended Reading**

- Why does Local Civic Cyber Resilience matter?
- The first parts of the Local Civic Cyber Resilience briefing are very good. The 10-steps and CiSP sections are for a different audience (Head of IT and Information Security Manager).
- Why your people are your most effective defence – (C-suite and potential of 'whaling')

**Useful Resources**

- Local Civic Cyber Resilience resources
- CPNI Passport to Good Security
- Local Civic Cyber Resilience knowledge bank - Leadership and Partnership

# Chief Executive

**Role**

1. Ultimately responsible for Local Civic Cyber Resilience

**Key Responsibilities**

1. Understand the need for Local Civic Cyber Resilience
2. Understand the potential impact of a cyber security incident or computer outage
3. Establish a Civic Cyber Resilience Group – Head of IT, Data Protection Officer, Local Resilience / Business Continuity Manager , Information Security Manager, Senior Information Risk Owner (SIRO)

**Recommended Reading**

- Why does Local Civic Cyber Resilience matter?
- The first parts of the Local Civic Cyber Resilience briefing are very good. The 10-steps and CiSP sections are for a different audience (Head of IT and Information Security Manager).
- Why your people are your most effective defence – (C-suite and potential of 'whaling')

**Useful Resources**

- Local Civic Cyber Resilience resources
- CPNI Passport to Good Security
- Local Civic Cyber Resilience knowledge bank - Leadership and Partnership

# Senior Information Risk Owner (SIRO)

**Role**

1. Own and oversee the implementation of the organisation's Cyber Resilience Strategy
2. Chair local cyber resilience group; represent Service Managers and escalate / cascade knowledge to/from these

**Key Responsibilities**

1. Work with the Local Resilience Manager and Business Continuity Manager to develop the organisation's Cyber Resilience Strategy
2. Arrange for a non-technical business-risk focussed strategic briefing delivered by DCLG/National Archives etc. for
    a. the Chief Executive / Board
    b. the local cyber resilience group members
    c. Service Managers and Information Asset Owners
3. Ensure all staff receive cyber awareness training
4. Develop and maintain an overview of
    a. data held, data flows (locations) and risks to data
    b. risk/threat to systems and likelihood of non-availability

**Recommended Reading**

- Why does Local Civic Cyber Resilience matter?
- The first parts of the Local Civic Cyber Resilience briefing are very good. The 10-steps and CiSP sections are for a different audience (Head of IT and Information Security Manager).

**Useful Resources**

- Local Civic Cyber Resilience resources
- CPNI Passport to Good Security
- Local Civic Cyber Resilience knowledge bank - Leadership and Partnership
- Why your people are your most effective defence

# Local Resilience Manager

**Role**

1. Together with the Business Continuity Manager, support the SIRO with the implementation of the organisation's Cyber Resilience Strategy
2. Lead on regional collaboration and joint working with other public service organisations, particularly through the Local Resilience Forum
3. Ensure resilience plans are tested regularly

**Key Responsibilities**

1. Understand the need for Local Civic Cyber Resilience
2. Understand the potential impact of a cyber security incident or computer outage
3. Develop local cyber civic resilience programme (support SIRO)
4. Together with Head of IT and Business Continuity Manager, consider if there are benefits of common / shared regional approach / loaned-staff (mutual aid) protocols / emergency response team etc. with peers from neighbouring authorities and other technology providers to public services within the locality.
5. Work with relevant Service Managers, Business Continuity Manager, Data Protection Officer and Information Security Manager to develop / source any specific training for staff in particularly sensitive areas – finance, social care and elections, for example. Such could come from DCLG, National Archives, National Cyber Security Centre (NCSC), DfE etc.
6. Participate in local Civic Cyber Resilience Group

**Recommended Reading**

- Why does Local Civic Cyber Resilience matter?
- Local Civic Cyber Resilience - learning from events
- Local Civic Cyber Resilience - thought leadership

**Useful Resources**

- Local Civic Cyber Resilience resources
- Why your people are your most effective defence
- CPNI Passport to Good Security
- Local Civic Cyber Resilience knowledge bank - Leadership and Partnership, Service Transformation and Community Resilience, Civil Contingency and Risk Management

# Business Continuity Manager

**Role**

1. Together with the Local Resilience Manager, support the SIRO with the implementation of the organisation's Cyber Resilience Strategy
2. Lead on staff training
3. Ensure business continuity plans are tested regularly

**Key Responsibilities**

1. Understand the need for Local Civic Cyber Resilience
2. Understand the potential impact of a cyber security incident or computer outage
3. Develop local cyber civic resilience programme (support SIRO)
4. Arrange a strategic briefing for the Chief Executive / Councillors by DCLG / National Archives etc. This should be about business risk and potential impact, and should not be technical nor focus on potential monetary fines. This should include:
    a. Why Cyber is one of four Tier One National Security Risks, alongside pandemic, terrorism, environmental etc. – potential impact:
        i. Disruption of services
        ii. Threat to service users' safety
        iii. Reputational damage
        iv. Post-event/breach resources required to demonstrate compliance
    b. The need for Local Civic Cyber Resilience
        i. Public services are increasingly reliant upon technology
        ii. The threat faced is more complex – human error / insider / physical / terrorist / espionage / criminal - targeted and/or opportunistic, computer enabled / computer dependent
        iii. Cyber incidents are high profile and attract significant media interest
        iv. Local public services are increasingly interconnected and interdependent
5. Arrange similar strategic briefings on cyber resilience for
    a. the local cyber resilience group members
    b. Service Managers and Information Asset Owners

6. Ensure all staff receive cyber awareness training
7. Ensure Service Managers have contingency plans in place covering lack of access to systems/data
8. Together with Head of IT and Local Resilience Manager, consider if there are benefits of common / shared regional approach / loaned-staff (mutual aid) protocols / emergency response team etc. with peers from neighbouring authorities and other technology providers to public services within the locality.
9. Work with relevant Service Managers, Data Protection Officer and Information Security Manager to develop / source any specific training for staff in particularly sensitive areas – finance, social care and elections, for example. Such could come from DCLG, National Archives, National Cyber Security Centre (NCSC), DfE etc.
10. Ensure cyber risks to service delivery are recorded corporately
11. Participate in local Civic Cyber Resilience Group

**Recommended Reading**

- Why does Local Civic Cyber Resilience matter?
- Local Civic Cyber Resilience - learning from events
- Local Civic Cyber Resilience - thought leadership

**Useful Resources**

- Local Civic Cyber Resilience resources
- Cyber Security e-learning - a suitable introductory learning for all – to access the course please use RDCCR as the username.
- Why your people are your most effective defence
- Future Learn, part of the Open University, offers a free Massive Open Online Course on Cyber Security aimed at protecting everyone (at home as well as at work) protect themselves online.
- CPNI Passport to Good Security
- Local Civic Cyber Resilience knowledge bank - Leadership and Partnership, Service Transformation and Community Resilience, Civil Contingency and Risk Management

# Service Managers & Information Asset Owners

## Role

1. Identify measures to minimise the impact of a cyber security incident or computer outage on service delivery and (customer) data

## Key Responsibilities

1. Understand the need for Local Civic Cyber Resilience
2. Understand the potential impact of a cyber security incident or computer outage
3. Understand data held, data flows (locations) and risks to data
4. Work with Head of IT and Information Security Manager to understand risk/threat to systems and likelihood of non-availability.
5. Work with Data Protection Officer, Local Resilience / Business Continuity Manager and Information Security Manager to develop / source any specific training for staff in particularly sensitive areas – finance, social care and elections, for example. Such could come from DCLG, National Archives, National Cyber Security Centre (NCSC), DfE etc.
6. Develop contingency plans in place covering lack of access to systems/data. Consider scenarios such as loss of computers, email, telephony or key systems for, for example, 2 hours, 2 days, 2 weeks, 2 months.
7. Develop and maintain details of data held, data flows (locations) and risks to data; ensure SIRO has an overview of these
8. Develop and maintain details of risk/threat to systems and likelihood of non-availability; ensure SIRO has an overview of these
9. Develop system recovery plan with Head of IT to understand how long systems might be unavailable
10. Test plans and processes regularly

## Recommended Reading

- Why does Local Civic Cyber Resilience matter?

**Useful Resources**

- Local Civic Cyber Resilience resources
- Local Civic Cyber Resilience knowledge bank - Service Transformation and Community Resilience

# Data Protection / Information Governance Officer

## Role

1. Ensure risks to sensitive data from cyber-attack are considered

## Key Responsibilities

2. Understand the need for Local Civic Cyber Resilience
3. Understand the potential impact of a cyber security incident or computer outage
4. Ensure a data loss / denial of access incident response plan is in place
5. Understand data loss / denial of access incident reporting / escalation processes (including outside the organisation)
6. Work with relevant Service Managers, Local Resilience / Business Continuity Manager and Information Security Manager to develop / source any specific training for staff in particularly sensitive areas – finance, social care and elections, for example. Such could come from DCLG, National Archives, National Cyber Security Centre (NCSC), DfE etc.
7. Ensure cyber risks to data held, data flows (locations) are recorded corporately
8. Participate in local Civic Cyber Resilience Group
9. Test plans and processes regularly

## Recommended Reading

- Why does Local Civic Cyber Resilience matter?

## Useful Resources

- Local Civic Cyber Resilience resources
- Local Civic Cyber Resilience knowledge bank - Information and Infrastructure

# Head of IT

## Role

1. Ensure cyber risks to core corporate IT and Service delivery systems are considered

## Key Responsibilities

1. Ensure a cyber incident response plan is in place with a single point of incident response management
2. Develop a plan for resilience of core corporate IT systems – data centre, email, internet access, networks, file storage
3. Work with Service Managers to help them understand risk/threat to their systems and likelihood of non-availability.
4. Develop a corporate system recovery plan with Service Managers including prioritising which systems are restored first etc.
5. Adopt the NCSC "10 Steps to Cyber Security"
6. Consider compliance / certification against key information security standards - ISO 27001, Cyber Essentials + etc.
7. Encourage Warning and Resource Point (WARP) and CiSP participation
8. Together with Local Resilience / Business Continuity Manager, consider if there are benefits of common / shared regional approach / loaned-staff (mutual aid) protocols / emergency response team etc. with peers from neighbouring authorities and other technology providers to public services within the locality.
9. Participate in local Civic Cyber Resilience Group
10. Ensure plans are tested regularly

## Recommended Reading

- Why does Local Civic Cyber Resilience matter?
- Local Civic Cyber Resilience briefing.
- Why your people are your most effective defence

**Useful Resources**

- Local Civic Cyber Resilience resources
- UK Government's 10 Steps to Cyber Security
- NCSC Advice & Guidance
- Cyber Essentials
- Cyber Information Sharing Platform (CiSP)
- What is a WARP?
- ISO 27001
- CPNI Passport to Good Security
- The Cyber Security and Information Assurance section in the GOV.UK Digital & Technical Skills manual
- Local Civic Cyber Resilience knowledge bank - Leadership and Partnership, Strategy, Security & Skills, Information and Infrastructure

# Information Security Manager

**Role**

1. Minimise the impact of a cyber security incident or computer outage on systems and (customer) data
2. Manage cyber incident reporting and escalation

**Key Responsibilities**

1. Ensure threat information sources are monitored
2. Manage compliance against ISO 27001, Cyber Essentials + etc.
3. Understand data loss / denial of access incident reporting / escalation processes (including outside the organisation)
4. Sign-up to the Government funded Cyber Information Sharing Platform (CiSP) which provides malware alerts, guidance and expert risk assessment
5. Join and participate in local Warning and Resource Point (WARP)
6. Develop strategic relations with regional Cyber Crime Unit and National Cyber Security Centre (NCSC)
7. Register emergency contact details with regional Cyber Crime Unit and National Cyber Security Centre (NCSC)
8. Sign up for free corporate monitoring tools from NCSC and others (e.g. Webcheck, www.haveibeenpwned.com)
9. Work with relevant Service Managers, Data Protection Officer and Local Resilience / Business Continuity Manager to develop / source any specific training for staff in particularly sensitive areas – finance, social care and elections, for example. Such could come from DCLG, National Archives, National Cyber Security Centre (NCSC), DfE etc.
10. Participate in local Civic Cyber Resilience Group
11. Test plans and processes regularly

**Recommended Reading**

- Why does Local Civic Cyber Resilience matter?
- Local Civic Cyber Resilience briefing.

**Useful Resources**

- Local Civic Cyber Resilience resources
- Local Civic Cyber Resilience resources
- UK Government's 10 Steps to Cyber Security
- NCSC Advice & Guidance
- Cyber Essentials
- Cyber Information Sharing Platform (CiSP)
- What is a WARP?
- Local Civic Cyber Resilience knowledge bank - Strategy, Security & Skills
- North East Regional Special Operations Unit (including North East Regional Cyber Crime Unit)

# Appendix 1: NORTH EASTERN ICT Partnership (NEICT)

NEICT is a partnership of the Heads of IT from

- Darlington Borough Council
- Durham County Council
- Gateshead Council
- Newcastle City Council
- Nexus – Tyne and Wear Passenmger Transport Executive
- North Tyneside Council
- Northumberland County Council
- South Tyneside Council
- Stockton Borough Council
- Sunderland City Council

It provides a safe environment for

- sharing and developing expertise, best practice, learning, skills and experience
- developing new, and exploiting existing ICT infrastructure, applications and developments
- working together to support efficiency, modernisation and shared services agendas
- maximising opportunities for jointly procuring ICT goods and services
- working with other organisations to ensure a coordinated approach to regional ICT developments and to help shape the use of ICT in the North East for the benefit of the residents, people who work here and those who visit the region

Much of NEICT's focus recently has been connecting our colleagues in council service delivery with the insight coming out of Central Government around information security especially because of Public Services Network compliance. The local information security network, ISNorthEast, and our series of 'Enabling Safe Business' events are part of this work.

# Appendix 2: ISNorthEast

ISNorthEast is the Warning, Advice & Reporting Point for the north east government community (NEGWARP).

ISNorthEast brings together the governance, assurance and security professionals from public sector organisations in Northumberland, Tyne and Wear, Durham and the Tees Valley in a trusted community.

It allows them to get together on a regular basis to share good practice, exchange views and address information assurance and cyber security issues facing local public service organisations that could potentially be affecting everyone.

Membership is open to information security and information assurance officers from non-profit public service organisations in the north east region and their outsourced delivery partners and is free of charge. Members from organisations outside the north east region may be admitted at the forum's discretion.

ISNorthEast holds quarterly half-day meetings in a central location where common issues are discussed, often with invited expert speakers. In addition to meetings, members receive a daily round up of threats, vulnerabilities and relevant news stories.

Critically, members have a mechanism to immediately alert each other of real threats being encountered in a sort of 'neighbourhood watch' for public data and systems.

ISNorthEast has a presence on the CiSP national cyber security platform and its members contribute to wider discussions on the platform including in the North East Region CiSP Group.

Current Members include:

| | |
|---|---|
| Local Government (councils) | 1. Durham County Council<br>2. Gateshead Council<br>3. Hartlepool Council<br>4. Middlesbrough Council<br>5. Newcastle Upon Tyne City Council<br>6. North Tyneside Council<br>7. Northumberland County Council<br>8. Redcar and Cleveland Borough Council<br>9. South Tyneside Council<br>10. Sunderland City Council<br>11. Xentrall ICT Services (Stockton BC & Darlington BC) |
| Local Government (other) | 12. BT South Tyneside<br>13. Engie (North Tyneside Council)<br>14. ICT Gateshead (schools curriculum support)<br>15. North Eastern ICT Partnership |
| Passenger Transport Executive | 16. Nexus |

| | |
|---|---|
| Central Government | 17. Department of Work and Pensions |
| | 18. HMRC |
| | 19. Homes and Communities Agency |
| Health | 20. County Durham and Darlington NHS Foundation Trust |
| | 21. Newcastle upon Tyne Hospitals NHS Foundation Trust |
| | 22. NHS Business Services Authority |
| | 23. NHS Protect |
| | 24. South Tyneside NHS Foundation Trust |
| Higher Education | 25. Durham University |
| | 26. Newcastle University |
| | 27. Teesside University |
| | 28. University of Sunderland |
| Police | 29. Cleveland Police |
| | 30. Durham Constabulary |
| | 31. Northumbria Police |
| | 32. North East Regional Cyber Crime Unit |
| Fire | 33. Tyne and Wear Fire & Rescue |
| Out of Area | 34. Calderdale Council |
| | 35. Edinburgh City Council |
| | 36. Hambleton District Council |
| | 37. Hull City Council |
| | 38. Kirklees Council |