NORFOLK RESILIENCE FORUM
preparing for emergencies

COVID-19

Cyber Delivery Group

Norfolk County Council

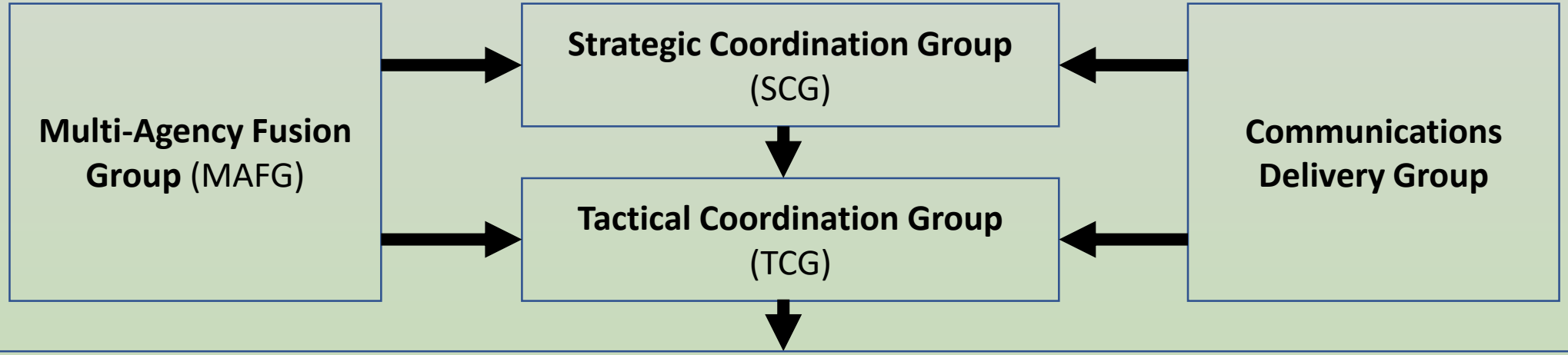
Civil Contingencies Act 2004

- Defines how the government prepares and plans for emergencies, working nationally, locally and co-operatively to ensure civil protection in the UK.

- The Act divides local responders into 2 categories, Category 1 (emergency services, local authorities, NHS bodies) and Category 2 (utility providers, transport providers, Health & Safety Executive, port authorities).

- In an emergency response, Category 1 and 2 organisations come together to form local resilience forums (which are based on geographic policing areas) to help co-ordination and co-operation between responders at the local level.

LRF – Command, Control & Coordination (C3 structure)
Response Phase



Delivery Groups

Self Isolation for Transient and Vulnerable Groups	Health and Social Care	Cyber Delivery Group	Mortality Pathway Coordination Group	Test Trace Track (TTT)
Domestic Violence	Community Resilience	Recovery	Economy	Social Distancing

Cyber Delivery Group Inception

This was the first time in the history of the Norfolk LRF that a cyber delivery group has been stood up as part of an emergency response.

The national emergency response for COVID-19 relates to a viral pandemic, why do we need a cyber delivery group?

The answer to that is **risk-**

- Loss of IT infrastructure is a significant risk identified within the LRF risk assessment for COVID-19.
- The National Cyber Security Centre assess that public sector organisations are likely to see an increase in targeted cyber attacks.
- The emergency response effort is heavily reliant upon digital systems and services across public sector organisations.
- Efficient and secure methods of data sharing, data analytics and communication are essential.
- A significant cyber incident impacting any one of our member organisations would have a catastrophic impact on the collective ability to deliver the required emergency response effort.

Cyber Delivery Group Structure

Delivery Group Lead

Local Authorities

- Borough Council of Kings Lynn & West Norfolk
- Broadland District Council
- Breckland District Council
- Great Yarmouth Borough Council
- Norfolk County Council
- North Norfolk District Council
- Norwich City Council
- South Norfolk District Council

Emergency Services

- East of England Ambulance Service
- ERS Medical
- Norfolk & Suffolk Constabulary

NHS

- James Paget Hospital
- Norfolk & Norwich University Hospital
- Queen Elizabeth Hospital
- Norfolk & Waveney CCG
- Norfolk & Suffolk NHS Foundation Trust

Cyber Delivery Group

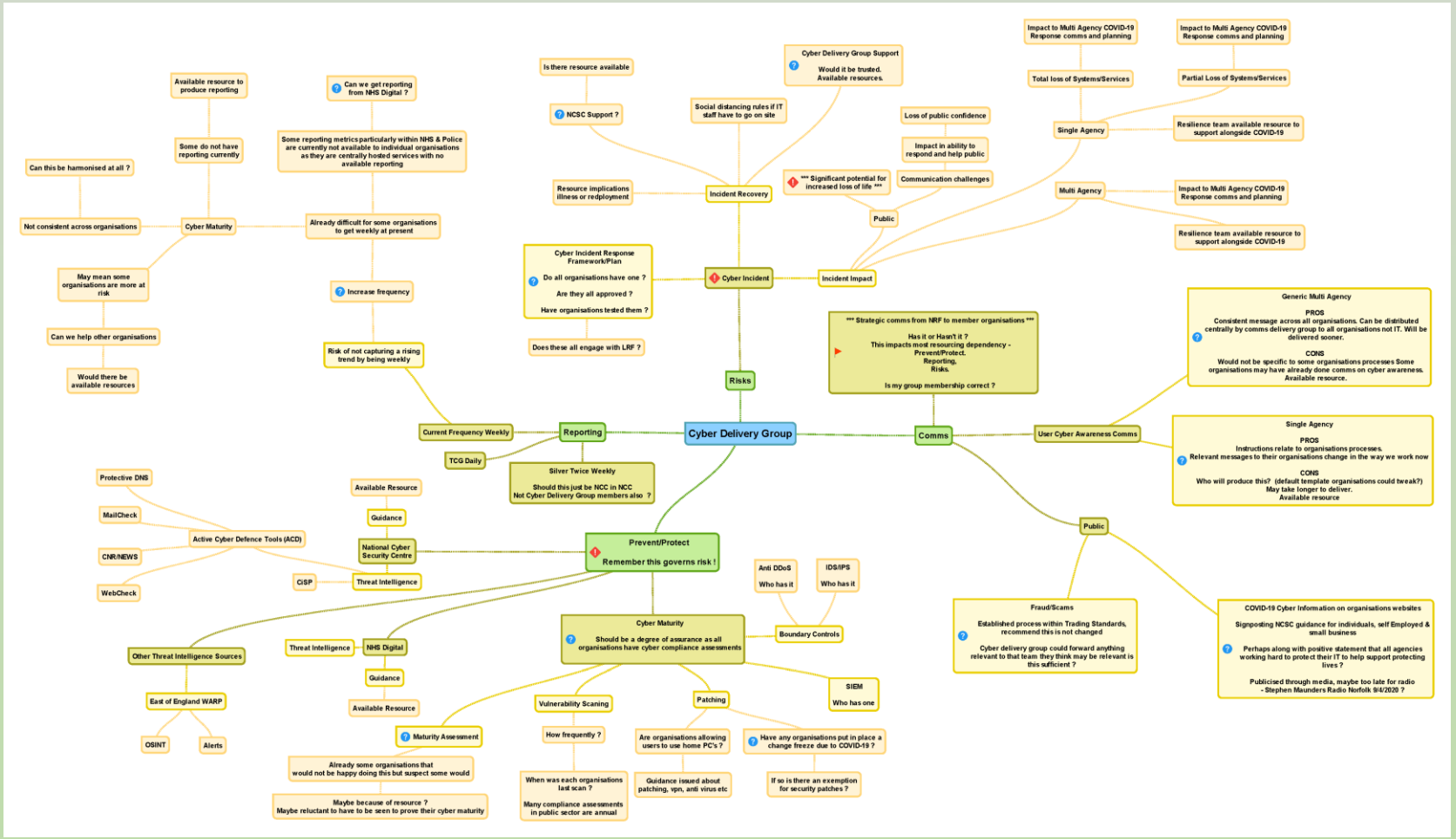
Terms of Reference

- Purpose (why) – To advise Strategic Command Group of cyber risk to COVID-19 planning response efforts.
- Outcome (what) – Regular updates to brief key stakeholders of cyber risk assessment.
- Approach (how) – Review regular reporting outputs from the delivery group member organisations IT systems security controls alongside cyber threat intelligence sources to inform the cyber risk assessment.

NORFOLK RESILIENCE FORUM
preparing for emergencies

Norfolk County Council

Cyber Delivery Group
Mind Mapping



Cyber Delivery Group

Security Control Reporting

The key objective of the delivery groups security control reporting is to collect and collate supporting evidence collected from IT infrastructure security controls from each organisation to inform and assess the level of cyber risk.

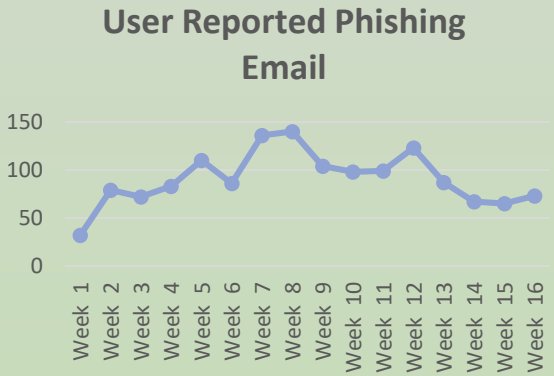
- Is any individual organisation or specific sector being targeted ?
- How effective are our perimeter security controls ?
- Are we observing an increase or decrease of suspicious activity ?
- Do we need to issue any specific cyber awareness communications to our users to reduce risk for a specific threat?

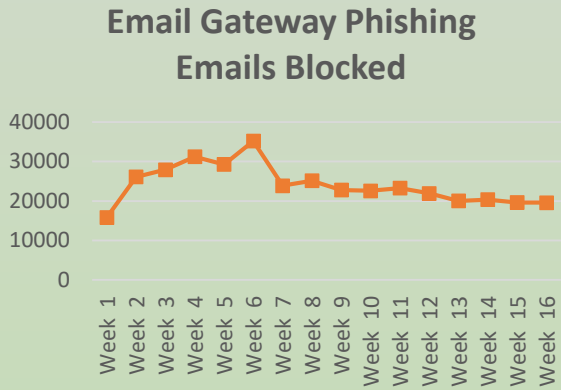
Cyber Delivery Group Reporting Outputs

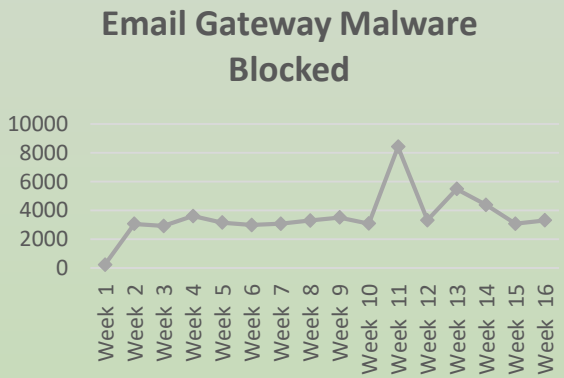
The graphs to the right show the weekly trending that is reported from IT security controls for all cyber delivery group member organisations.

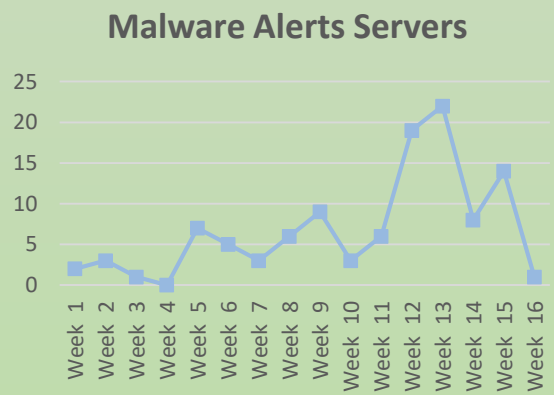
The trend reports are circulated to key stakeholders weekly and provide valuable intelligence on cyber threat.

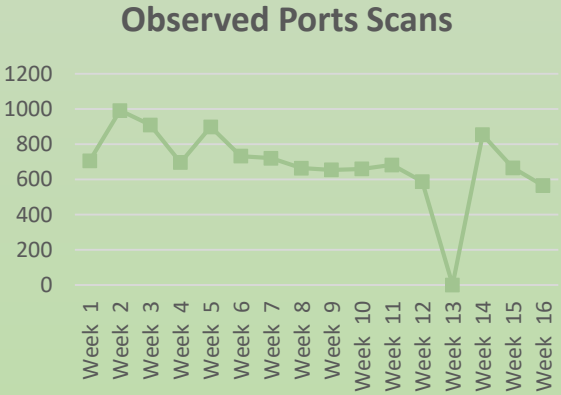
These are also reported by specific sector (local authority, acute hospital, emergency services and community health).

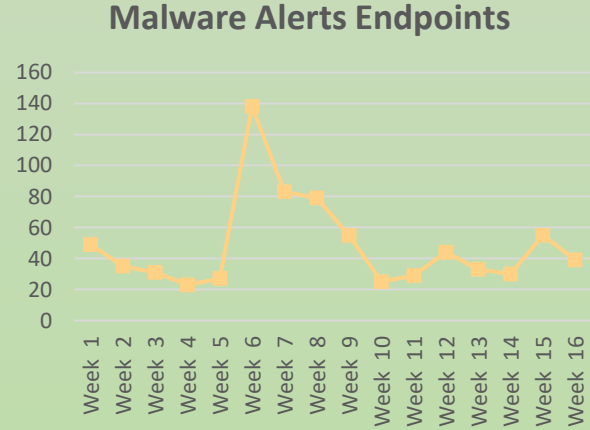












Cyber Delivery Group

Threat Intelligence

Prevent and protect are two pivotal components to manage and mitigate cyber risk.

The delivery group has access to a number of threat intelligence sources which are monitored on a continual basis. Threat intelligence sources provide valuable insight into known exploits, software supplier security patches and enables us to take preventative measures to protect our IT systems and services from threat actors.

Threat intelligence sources monitored by the group include:

- The National Cyber Security Centre Advisories and CiSP.
- US-Cert.
- NHS CareCERT.
- NLAWARP.
- CyberShare.

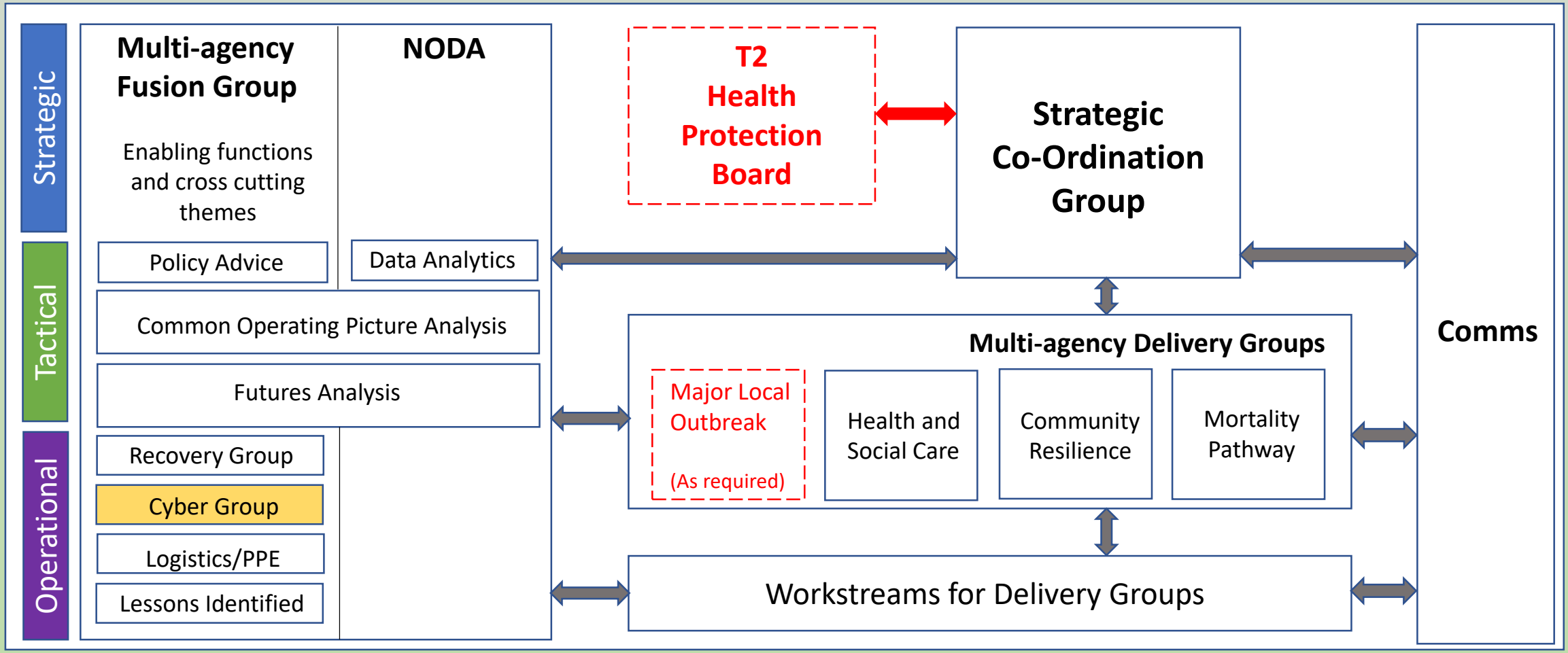
Recovery Phase Transition

What's Changed?

Very little:

- Delivery group structure and membership remains the same.
- Battle rhythm has been relaxed from weekly to fortnightly.
- We continue to provide and share weekly reporting.
- We continue to share threat intelligence and discuss new vulnerabilities.
- We simply report into a different structure once a week.

LRF – Command, Control & Coordination (C3 structure)
Recovery Phase



Cyber Delivery Group

Positive Outcomes

The inception of the Norfolk Cyber Delivery Group has created many positive outcomes:

- It is Norfolk's first public sector collaboration to focus on cyber risk management.
- It will enable the sharing, development and adoption of consistent cyber risk management best practice.
- Increased the visibility and awareness of cyber threats within individual organisations, sector and locality.
- Created an appetite to continue the public sector cyber collaboration in Norfolk post COVID-19.
- Created an active forum for the sharing of information relating to cyber security threats and emerging vulnerabilities.

Cyber Delivery Group

Future Opportunities

Having an established cyber security community across public sector services in Norfolk introduces a number of opportunities to increase both cyber maturity and resilience in our locality:

- Peer support – With the right agreements in place, there is a real opportunity to share resources across organisations and sectors to help public sector organisations in our locality recover from any future cyber security incidents more efficiently.

- Sharing of cyber security incident intelligence (IOC's & attack chains) will facilitate an increased ability to contain an incident and prevent a wider impact across public sector services where in some cases minutes really do matter.

- Increased visibility of cyber security threats and risk for public sector services that can be shared with wider regional and national bodies such as the WARPs and national Cyber Security Centre.

- Further development and automation of cyber security reporting to enable increased frequency and additional content to increase capability and intelligence.

- Develop and use areas of expertise within local public sector services such as pen testing to provide more frequent testing and assurance of our IT systems to facilitate an increase in cyber resilience and reduce both risk and cost.

Cyber Delivery Group

Lessons Identified

Lessons identified is a critical component to drive improvement:

- Strategic Directive to stand up the delivery group was not well communicated or understood within all public sector organisations which introduced conflict with organisational strategy.
- Cyber maturity is very different within the delivery group member organisations. Some organisations have full time cyber security roles, for others this is an additional responsibility for other existing IT roles. At a regional level, there is a significant amount of opportunity to help each other to raise our maturity at both an organisational and regional level.
- Wider collaboration and sharing of security reporting increases our ability to understand and manage cyber security risk and is something we need to continue to develop, deliver and scale.