LRG Update – Cyber Newsletter, February 2020

The lead officers for the London Resilience Partnership Cyber Incident Response Capability in London have published this newsletter, in consultation with the London Resilience Group. It provides an overview for local authorities and businesses, as to the work being done in London to enhance our cyber incident preparedness, as well as sharing some lessons learned from recent exercises. We have highlighted some resources and available training and exercising opportunities.

1. National Cyber Security Strategy 2016-2021

The National Cyber Security Programme 2016/21 has three core elements to ensure that we are secure and resilient to cyber threats, prosperous and confident in the digital world.

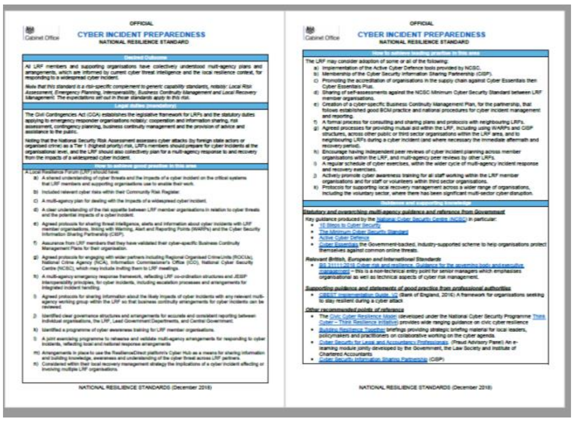
'Cyber security' refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures (The National Cyber Security Strategy 2016-2021).'

2. National Cyber Security Centre (NCSC)

NCSC is the lead government department for managing cyber risk. However, depending on the type of incident, law enforcement agencies might be prominent in the response such as Action Fraud and Regional Organised Crime Units.

NCSC supports the most critical organisations in the UK, the wider public sector, industry and SMEs, by providing information, advice and guidance on cyber security management.. When incidents do occur, they provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future. For more information, please see https://www.ncsc.gov.uk.

3. Cyber Incident Preparedness; National Resilience Standard



OFFICIAL

Cabinet Office

CYBER INCIDENT PREPAREDNESS
NATIONAL RESILIENCE STANDARD

Desired Outcome

All LRF members and supporting organisations have collectively understood multi-agency plans and arrangements, which are informed by current cyber threat intelligence and the local resilience context, for responding to a widespread cyber incident.

Note that this standard is a risk-specific complement to generic capability standards, notably: Local Risk Assessment, Emergency Planning, Interoperability, Business Continuity Management and Local Recovery Management. The expectations set out in those standards apply to this risk.

Legal duties (mandatory)

The Civil Contingencies Act (CCA) establishes the legislative framework for LRFs and the statutory duties applying to emergency responder organisations notably: cooperation and information sharing, risk assessment, contingency planning, business continuity management and the provision of advice and assistance to the public.

Noting that the National Security Risk Assessment assesses cyber attacks (by foreign state actors or organised crime) as a Tier 1 (highest priority) risk, LRFs members should prepare for cyber incidents at the organisational level, and the LRF should also collectively plan for a multi-agency response to and recovery from the impacts of a widespread cyber incident.

How to achieve good practice in this area

A Local Resilience Forum (LRF) should have:

a) A shared understanding of cyber threats and the impacts of a cyber incident on the critical systems that LRF members and supporting organisations use to enable their work.
b) Included relevant cyber risks within their Community Risk Register.
c) A multi-agency plan for dealing with the impacts of a widespread cyber incident.
d) A clear understanding of the risk appetite between LRF member organisations in relation to cyber threats and the potential impacts of a cyber incident.
e) Agreed protocols for sharing threat intelligence, alerts and information about cyber incidents with LRF member organisations, linking with Warning, Alert and Reporting Points (WARPs) and the Cyber Security Information Sharing Partnership (CiSP).
f) Assurance from LRF members that they have validated their cyber-specific Business Continuity Management Plans for their organisation.
g) Agreed protocols for engaging with wider partners including Regional Organised Crime Units (ROCUs), National Crime Agency (NCA), Information Commissioner's Office (ICO), National Cyber Security Centre (NCSC), which may include inviting them to LRF meetings.
h) A multi-agency emergency response framework, reflecting LRF co-ordination structures and JESIP interoperability principles, for cyber incidents, including escalation processes and arrangements for integrated incident handling.
i) Agreed protocols for sharing information about the likely impacts of cyber incidents with any relevant multi-agency working group within the LRF so that business continuity arrangements for cyber incidents can be reviewed.
j) Identified clear governance structures and arrangements for accurate and consistent reporting between individual organisations, the LRF, Lead Government Departments, and Central Government.
k) Identified a programme of cyber awareness training for LRF member organisations.
l) A joint exercising programme to rehearse and validate multi-agency arrangements for responding to cyber incidents, reflecting local and national response arrangements.
m) Arrangements in place to use the ResilienceDirect platform's Cyber Hub as a means for sharing information and building knowledge, awareness and understanding of the cyber threat across LRF partners.
n) Considered within their local recovery management strategy the implications of a cyber incident affecting or involving multiple LRF organisations.

NATIONAL RESILIENCE STANDARDS (December 2018)

OFFICIAL

Cabinet Office

CYBER INCIDENT PREPAREDNESS
NATIONAL RESILIENCE STANDARD

How to achieve leading practice in this area

The LRF may consider adoption of some or all of the following:

a) Implementation of the Active Cyber Defence tools provided by NCSC.
b) Membership of the Cyber Security Information Sharing Partnership (CiSP).
c) Promoting the accreditation of organisations in the supply chain against Cyber Essentials then Cyber Essentials Plus.
d) Sharing of self-assessments against the NCSC Minimum Cyber Security Standard between LRF member organisations.
e) Creation of a cyber-specific Business Continuity Management Plan, for the partnership, that follows established good BCM practice and national procedures for cyber incident management and reporting.
f) A formal process for consulting and sharing plans and protocols with neighbouring LRFs.
g) Agreed processes for providing mutual aid within the LRF, including using WARPs and CiSP structures, across other public or third sector organisations within the LRF area, and to neighbouring LRFs during a cyber incident (and where necessary the immediate aftermath and recovery period).
h) Encourage having independent peer reviews of cyber incident planning across member organisations within the LRF, and multi-agency peer reviews by other LRFs.
i) A regular schedule of cyber exercises, within the wider cycle of multi-agency incident response and recovery exercises.
j) Actively promote cyber awareness training for all staff working within the LRF member organisations and for staff or volunteers within third sector organisations.
k) Protocols for supporting local recovery management across a wider range of organisations, including the voluntary sector, where there has been significant multi-sector cyber disruption.

Guidance and supporting knowledge

Statutory and overarching multi-agency guidance and reference from Government

Key guidance produced by the National Cyber Security Centre (NCSC) in particular:

- 10 Steps to Cyber Security
- The Minimum Cyber Security Standard
- Active Cyber Defence
- Cyber Essentials the Government-backed, industry-supported scheme to help organisations protect themselves against common online threats.

Relevant British, European and International Standards

- BS 31111:2018 Cyber risk and resilience. Guidance for the governing body and executive management – this is a non-technical entry point for senior managers which emphasises organisational as well as technical aspects of cyber risk management.

Supporting guidance and statements of good practice from professional authorities

- CBEST Implementation Guide, V2 (Bank of England, 2016) A framework for organisations seeking to stay resilient during a cyber attack

Other recommended points of reference

- The Civic Cyber Resilience Model developed under the National Cyber Security Programme Think Cyber – Think Resilience initiative provides wide ranging guidance on civic cyber resilience
- Building Resilience Together briefings providing strategic briefing material for local leaders, policymakers and practitioners on collaborative working on the cyber agenda.
- Cyber Security for Legal and Accountancy Professionals. (Fraud Advisory Panel) An e-learning module jointly developed by the Government, the Law Society and Institute of Chartered Accountants
- Cyber Security Information Sharing Partnership (CiSP)

NATIONAL RESILIENCE STANDARDS (December 2018)

“The UK now faces an increasing number of state and non-state groups with the ability and desire to carry out attacks using cyberspace (National Risk Register cyber assessment).” As part of the set of National Resilience Standards, a new Local Resilience Forum focused cyber incident preparedness standard has been developed in association with the National Cyber Security Centre. This standard describes legal obligations, good practise and leading practice examples of cyber incident preparedness options, and supplementary guidance and advice sources. Key themes include cyber awareness for staff, including cyber risks on risk registers, using available cyber defence tools provided by the NCSC, creating cyber incident specific BCM plans and developing a cyber exercise program. A copy of this standard can be found on the ResilienceDirect extranet (access to ResilienceDirect is for LRF partners only).

4. Cyber Capability Assessment – London Resilience Forum (LRF)

The capability assessment process provides an indicator of the maturity of London’s emergency response capabilities with each assessed against the criteria: doctrine; plans; resources and logistics; training; exercising; interoperability. The current lead agencies for the cyber response capability are NHS England and NHS Improvement (London) , and the City of London Corporation. Through this assessment process it has been agreed that a primary area of focus for London is to develop the Cyber Technical Advice Cell (C-TAC) concept. The C-TAC is a multi-agency cell, with the function to provide timely, coordinated and actionable advice to the Strategic Coordinating Group (similar to Scientific and Technical Advice Cell arrangements). Work is moving forward to develop this concept, including who should be involved in a C-TAC, information sources and facilities that they may require. This project is progressing as part of the LRF work programme. Further information is available in the London City Resilience Strategy under the section: Cyber Emergency Response Capability.

5. Resources for Businesses and the Public Sector

Cyber Griffin is an initiative that helps businesses and individuals in the Square Mile to protect themselves from **cyber** crime. Delivered by the City of London Police, they offer four key services, free of charge, across London. These services cover an immersive Lego table-top exercise, cyber incident response training, a cyber capability assessment, and informative ‘baseline briefings,’ for raising staff awareness and knowledge. Services are designed to be accessible to everyone, whether they have very little knowledge of cyber crime, or are individuals who hold IT security and risk management roles. For further information, please see https://cybergriffin.police.uk.

6. Where do I report a cyber incident?

If you find yourself subject to any type of cyber attack, where your systems have been accessed in an unauthorised manner, and you suspect private data may have been accessed, or your systems altered in any way, consider notifying the following:

1. Information Commissioners Office
2. National Cyber Security Centre
3. Shared services providers, or partners joined through your networks

7. Five learning tips from recent incidents and live cyber exercising

Cyber attacks can pose difficult decision making dilema, incur significant recovery costs, and bring fines for organinsations that are found to have been partly liable through a lack of protection and preparedness. The following points are key pieces of learning from both cyber attacks on essentail public services, and innovative live exercising in the cyber space.

1. Have a Ransomware Policy in Place

- It is a hard and heavy discussion to have when your business is crumbling around you. Make the decision in advance and then take it from there when the real thing happens.

2. Lets Talk Insurance

- Cyber attack-specific insurance is available, don’t just assume you have it. Furthermore, there are different types of cover available, and some packages include pre-event advice from specialists as part of avoiding an attack altogether, because they can be so costly.

3. Do a Hypothetical Impact Assessment In Advance

- Include the possibility of a ‘total loss of IT systems.’ You need to know how long a network rebuild will take, to avoid senior staff getting frustrated if they don’t understand why a system cannot simply be turned off and on again, as well as st implications. Be sure to assess critical services, assets and partners.

4. Cut the Jargon for Senior Managers

- When explaining the situation, have IT staff avoid product names like ' X applications.' Instead, talk about the services lost in terms that the users will understand, such as, 'access to email and diaries through outlook on all company owned devices have been lost'. This can make for quicker, clearer, less ‘tech-heavy’ conversations when you are under time pressure.

5. Manage Expectations

- The idea of having no systems for weeks on end is simply intangible for senior leaders, but nevertheless, this might be what is going to happen. Be clear about what can and cannot be done, including time-frame for diagnosing what the cyber incident actually is and what damage it has and could continue to do.

The London Resilience Group supports the work of the London Resilience Partnership in preparing for, and responding to emergencies. We are hosted by the London Fire Brigade.