Department for Levelling Up,
Housing & Communities

Response and Recovery Planning

V1.0

LOCAL DIGITAL Cyber

Objective

- Incidents will invariably happen. When they do, Councils should be prepared to deal with them and have mechanisms in place that minimise the impact on essential functions.

- The particular mechanisms required should be determined as part of the Council's overall risk management approach.

- Councils should make sure that they understand any mandatory incident reporting requirements that apply to them and include such requirements in their incident management planning.

LOCAL DIGITAL Cyber

Preparing an Incident Response Plan

- You should ensure that your Council's incident response plans are formed from a comprehensive risk assessment.
- Response plans should prioritise essential functions, and the assets and systems required to ensure their continued effective operation.
- Your cyber incident response plans should link to other business response functions.
- Form a cyber response team capable of implementing the plan, with the appropriate skills, tools and reach into other parts of your Council.
- The plan should cover all relevant potential incidents. It should be auditable and testable (via exercises) across a range of incident scenarios.

LOCAL DIGITAL Cyber

Preparing an Incident Response Plan – Continued…

- Test scenarios should draw on threat intelligence, past incidents, exercises and the ways in which security capabilities (e.g. security monitoring and alerting) would feature in your response options.

These scenarios could include, but not limited to:

- Ransomware / Malware Infection
- Hacker infiltration
- An inability to view status of the network or operational system
- System backup and restore
- Denial of Service
- An insider incident
- Emergency patching or AV signature roll-out
- Confirmation of normal operations

- Plans should articulate clear governance frameworks and roles with procedures for reporting to relevant internal or external stakeholders.

LOCAL DIGITAL Cyber

Preparing an Incident Response Plan – Continued…

- Plans should also set out a comprehensive range of containment, eradication and recovery strategies, specifying how and when they should be used.
- You should run exercises to test your ability to respond to incidents. These exercises should reflect past experience, red-teaming/scenario planning, or threat intelligence.
- Exercises should record lessons learned, covering governance, roles and internal communication, containment and recovery strategies.
- For further guidance - section 2 of the NIST Computer Security Incident Handling Guide, Part 4 of CREST Cyber Security Incident Response Guide or the Prepare section of ISO 27035.

LOCAL DIGITAL Cyber

Response and Containment

- The Council's security monitoring function should be capable of alerting with enough detail for a response team to triage.
- Eventualities not covered in the plan should be dealt with by risk-based decisions, taking account of factors like potential disruption, cost-effectiveness of response and the need for evidence preservation.
- Incidents should be reported to the appropriate internal and external authorities.
- The response team should be capable of prioritising incidents, according to the potential consequences and possible adverse impact on essential functions, using risk-based methods.

LOCAL DIGITAL Cyber

Response and Containment – Continued …

- Councils should seriously consider voluntarily reporting cyber security incidents to the NCSC, who may be able to provide situational awareness, drawing on incident reporting from other victims, as well as response and protective security advice.

- Further guidance is found in Section 3 of NIST Computer Security Incident Handling Guide, Part 5 of CREST Computer Security Incident Response Guide or Part 4 of ISO 27035.

LOCAL DIGITAL Cyber

Department for Levelling Up,
Housing & Communities

Lessons Learned

LOCAL DIGITAL Cyber

Objective

- When an incident does occur, it is important your Council learns lessons as to why it happened and, where appropriate, takes steps to prevent the issue from reoccurring.

- Address the root cause or systemic problems, rather than to fix a narrow issue. For example, to address the Council's overall patch management process, rather than to just apply a single missing patch.

LOCAL DIGITAL Cyber

Root Causes and Shortfall

- Each incident or exercise should include an assessment of the root causes and any other factors.
- Council's should consider what measures would need to be in place to prevent similar incidents in the future or to improve the response capabilities.
- Improving the timeliness of detection, or introducing mitigations to reduce the likelihood of such incidents occurring.
- Council's should produce good quality reporting during incident response and exercising.

LOCAL DIGITAL Cyber

Root Causes and Shortfall - Continued …

- Keep detailed records to show how information was used to make decisions.
- Root causes of an incident must be identified so any shortfalls in response and preventive strategies can be assessed.
- Examples might include gaps in security monitoring, poor understanding of networks, insufficient business continuity planning, or inadequate internal communication.
- Lessons should be clearly and comprehensively documented and fed into the Council's response plans. Further details can be found in Sections 3.1-2 of NIST Computer Security Incident Handling Guide, Part 5 of CREST Computer Security Incident Response Guide and parts 2-3 of ISO 27035.

LOCAL DIGITAL Cyber

Reduced Risk

- Use post-incident and post-exercise reviews to actively reduce the risks associated with the same, or similar, incidents happening in future.
- Lessons learned can inform any aspect of the Council's cyber security, including:
  - System configuration
  - Security monitoring and reporting
  - Investigation procedures
  - Containment/recovery strategies
  - Governance and communication around incident management

LOCAL DIGITAL Cyber

Reporting

- Lessons drawn from incidents or exercising should be shared with all relevant internal and external stakeholders.

- Examples might include, regulators and competent authorities, internal governance or organisations such as NCSC.

LOCAL DIGITAL Cyber

Data Retention

- Many incidents go undetected for long periods. You should consider your Council's data retention policies, especially the retention period and quality of historical data to meet legal or regulatory requirements.

- In determining adequate retention periods, you should consider how effective the Council’s monitoring capability is, experience of past incidents and any examples available in threat intelligence.

- When an incident occurs, the Council should have sufficient data to perform the required level of post-incident analysis, learn lessons from the analysis, and report the right details to the right people.

LOCAL DIGITAL Cyber

Staying in touch - cyber support sessions

Cyber treatment plan & implementation support session available to book using this link: https://calendly.com/andrea-baron/ad-hoc-call-with-council .
These are longer 1:1 sessions between DLUHC cyber team and a council, available for any support, guidance or hands on help for the implementation of your cyber treatment plan.

Cyber support drop in sessions every Wednesday for 30 minute session between 2pm - 4pm. These regular 1:1 sessions are available for you to book anytime using the Calendly link: https://calendly.com/andrea-baron/drop-in-support-session .

Cyber clinics are occurring on the 3rd Thursday of the month between 11.30am - 12.30pm where a targeted cyber focus area will be presented, tool sets demonstrated and will be open to questions. Support, guidance and hands-on help is available to assist you in adoption and implementation.

LOCAL DIGITAL Cyber

Department for Levelling Up,
Housing & Communities

Thank you

We welcome feedback on our cyber support service

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

LOCAL DIGITAL Cyber