Department for Levelling Up,
Housing & Communities

Incident Management & Business Continuity/ Disaster Recovery

V1.0

LOCAL DIGITAL Cyber

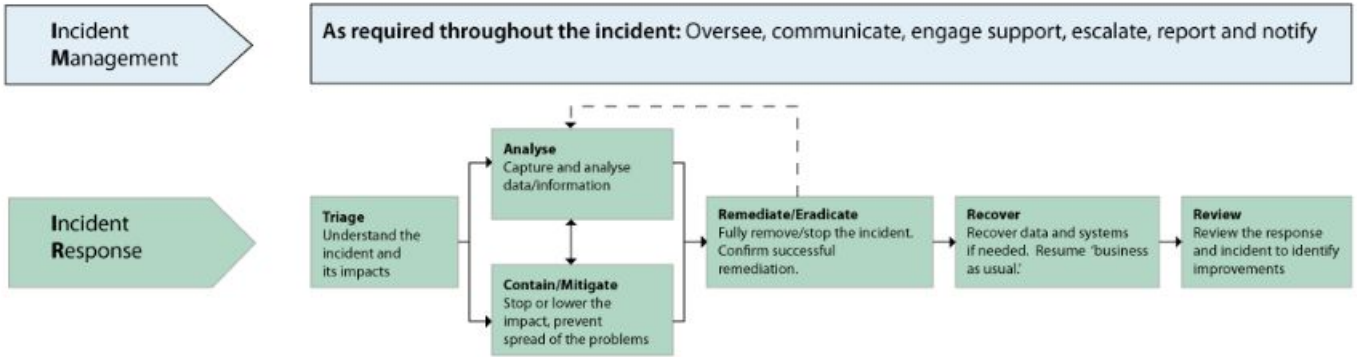
What is Incident Management?

Incident management is the process of effectively responding to an unplanned event

The NCSC defines a cyber security incident as:

- A breach of a system's security policy in order to affect its integrity or availability
- The unauthorised access or attempted access to a system

Incident Response (IR) Is the set of procedures used to deal with the impact of a s ments to work t



LOCAL DIGITAL Cyber

Benefits of Incident Management

- Having effective incident management in place reduces the impact of a cyber incident
- A documented and trained plan will help staff make appropriate decisions
- In the event of an incident, a timely managed response, with clear communication throughout allows Interested parties to have trust in the Council
- Gaps and issues can be Identified in the response capability

LOCAL DIGITAL Cyber

Incident Response Lifecycle

- Preparation
- Detection and Analysis
- Containment
- Eradication and Recovery
- Post-Event Activity

LOCAL DIGITAL Cyber

Incident Response Plan

A basic incident response plan should include:

- Key contacts
- Escalation criteria
- Basic flowchart or process showing the full Incident life-cycle
- At least one conference number
- Basic guidance on legal or regulatory requirements

LOCAL DIGITAL Cyber

Roles and Responsibilities

- Clearly documented in appropriate plans
- Fully understood
- Individuals should carry out their responsibilities
- It has been recognised that this Is a challenge and actions are In place to aid

LOCAL DIGITAL Cyber

Business Impact Assessment (BIA)

- A BIA is used to identify the Council's critical systems
- A BIA is the process of determining the criticality of business activities to ensure operational resilience and continuity of operations during and after a business disruption
- **Recovery Time Objective** (RTO) – maximum amount of time to restore normal operations
- **Recovery Point Objective** (RPO) – maximum amount of data the Council can tolerate losing

LOCAL DIGITAL Cyber

Incident Identification

- **Technical:** Alerts from monitoring tools e.g. SIEMs and AV/IDS alerts
- **Staff:** Users report incidents when there is any suspicious activity e.g. unusual email
    - It is important that suspicious activity Is reported and local Council responses are known
- **Third Parties:** Those who perform Incident investigations and threat research

LOCAL DIGITAL Cyber

Triaging an Incident

- Determine the type of incident (category) and the severity:
  - Confidentiality
  - Integrity
  - Availability
- Category type examples:
  - Phishing
  - Unauthorised access
  - Insider threat
  - Data breach

LOCAL DIGITAL Cyber

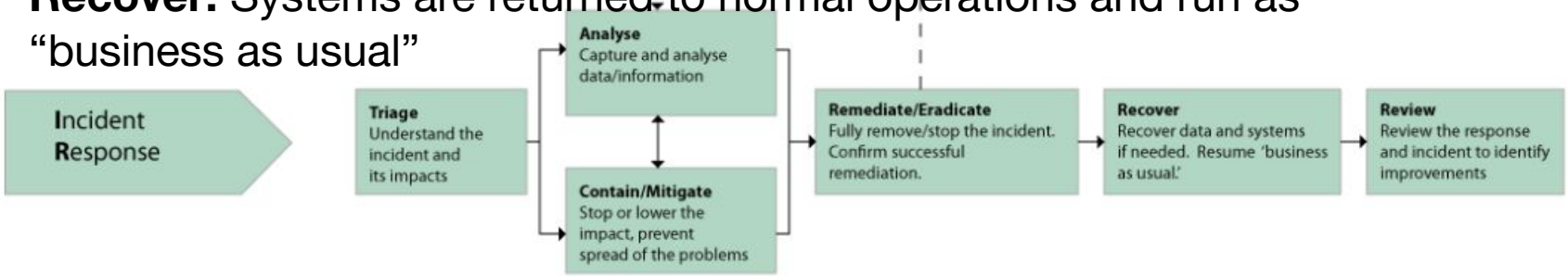
Severity - Examples

- Over 80% of staff (or several critical staff/teams) unable to work
- Critical systems offline with no known resolution
- High risk to / confirmed breach of sensitive client or personal data
- Financial Impact of £[TBC]
- Severe reputational damage - likely to Impact business long term

LOCAL DIGITAL Cyber

Responding to an Incident

- **Analyse:** Analysis of any relevant data/information
- **Contain/Mitigate:** Aim to reduce the impact of the incident by containing and preventing it from spreading
- **Remediate/Eradicate:** Fully remove or quarantine the Incident from the network and systems
- **Recover:** Systems are returned to normal operations and run as "business as usual"



Incident Management - During an Incident

- Tracking, documenting, assigning and correlating all findings, tasks and communications
- Arranging regular update meetings
- Escalating serious Incidents to senior management
- Ensuring the incident is communicated appropriately
- Ensuring the full Incident lifecycle is covered

LOCAL DIGITAL Cyber

Lessons Identified

- A post incident review will help identify the positives, negatives and areas for improvement
- The review applies to the incident itself and also the Council's response to the Incident
- Understanding lessons identified will help Identify gaps in the process to be addressed

LOCAL DIGITAL Cyber

Templates/Documents

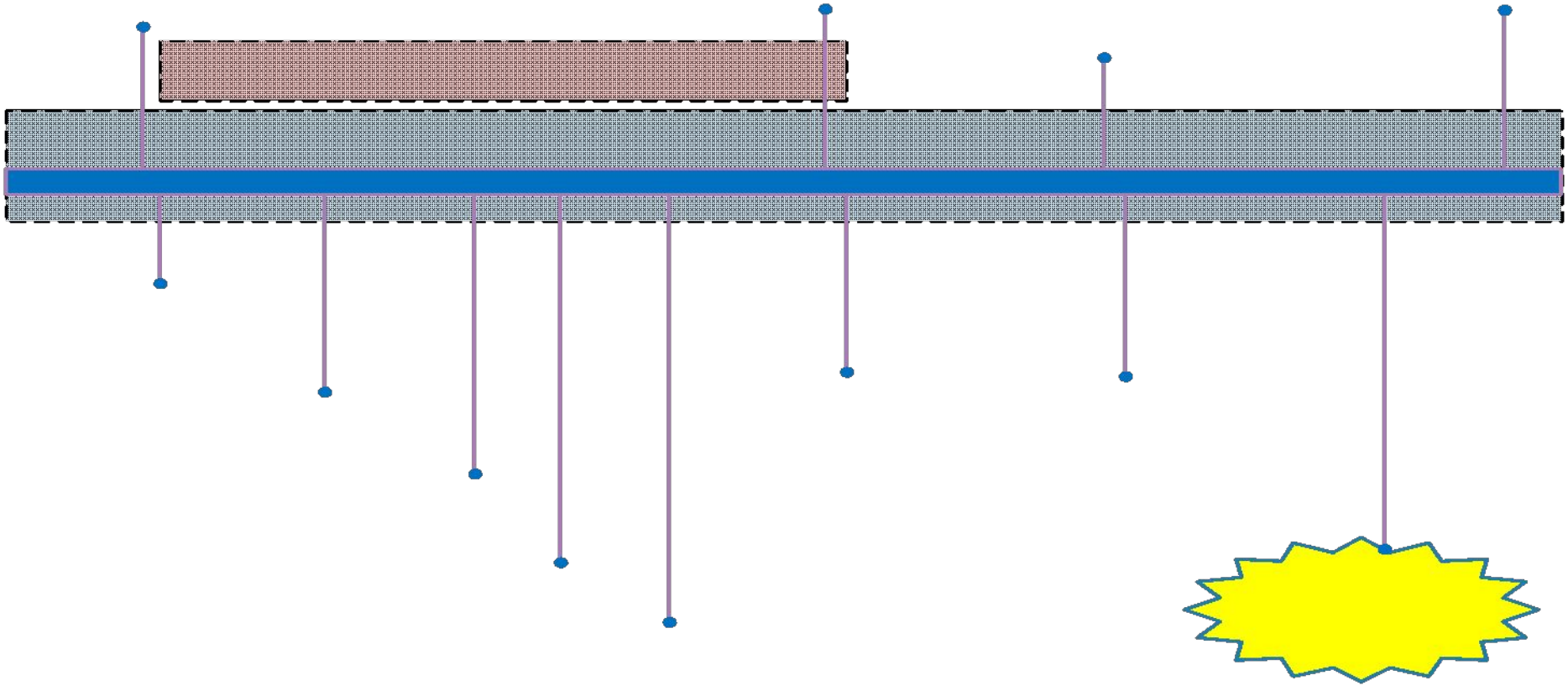
- IT Disaster Recovery Plan and Process Guide
- BIA Template
- BCP Template
- Overview of RTO and RPO
- Response and Recovery Planning

LOCAL DIGITAL Cyber

Copeland Council - Ransomware

- Copeland Council were subject to a zero day ransomware attack in 2017
- Three days after the attack, the majority of Copeland Council's files had been encrypted by the ransomware
- Everything had to be rebuilt – twice
- Ransom to decrypt files was Bitcoin payment
- Parts of the Council spent around 10 weeks without basic IT functionality

LOCAL DIGITAL Cyber



LOCAL DIGITAL Cyber

What is Business Continuity & Disaster Recovery? (BCDR)

- Set of processes and techniques used to help a Council recover from a major incident/disaster and continue or resume business operations
- BCDR combines IT and Council operations in the aftermath of a disaster
- Business Continuity aims to ensure Council services continue
- Disaster Recovery aims to recover from the disaster
- An Incident may cause disruption to normal Council operations which results In the business continuity plan being Invoked

LOCAL DIGITAL Cyber

Importance of testing BC/DR Plans

- Assesses the Councils ability to respond to incidents that could affect the operation of essential functions/services
- Allows exercises to reflect on past experience, scenario planning, or threat intelligence
- Enabling the Council to understand the complexity of the IT Recovery processing In terms of:
    - Services that are prerequisites to a recovery, e.g. networks, storage, DNS, AD
    - The personnel and skills required to be available to perform recovery
    - Confirming If recovery is possible within targeted RPO & RTO

LOCAL DIGITAL Cyber

Testing of BCDR

- Walkthrough Testing
- Simulation Testing
- Parallel Testing
- Full Interruption Testing

LOCAL DIGITAL Cyber

BCDR Plan

A BCDR plan should include:

- Business Impact Assessment including Recovery Point Objective (RPO) and Recovery Time Objective (RTO)
- Backup Strategy
- Roles and Responsibilities
- Contacts
- BCP and DRP Procedures

LOCAL DIGITAL Cyber

Exercise in a Box (EiaB)

- NCSC's tool to help test and practise the response to a cyber attack
- Enables a Council to walkthrough an entire incident
- EiaB looks at the incident management and the BCDR
- Ransomware Is one scenarios option that can be selected
- Other EiaB scenarios can be found here

LOCAL DIGITAL Cyber

Summary

- Incident Management life-cycle: Preparation; Detection and Analysis; Containment; Eradication and Recovery; Post-Event Activity
- Effective incident management reduces the impact, helps staff make informed decisions, allows for clear communication and Identified any gaps or issues in the response capability
- BCP testing is important; Ransomware incidents can be tested using NCSC's Exercise In a Box
- Many related templates can be found within this presentation

LOCAL DIGITAL Cyber

Staying in touch

Follow our progress

- Read our fortnightly sprint notes on Medium
- Follow LDCU on Twitter (@LDgovUK)
- Subscribe to our Cyber newsletter for progress updates and news relevant to those working in and around local government cyber security
- We'll also be sharing regular updates on the DLUHC Digital blog

Have your say

We welcome further collaboration and Input, so if you would like to share with us any strong evidence to support our research please email cybersupport@localdigital.gov.uk.

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