SECURE CONNECTED PLACES

INCIDENT RESPONSE

Department for Science, Innovation & Technology

In collaboration with

plexal DAINTTA Configured THINGS

WHAT WILL I GET OUT OF USING THIS RESOURCE?

All connected systems are vulnerable to cyber incident, which can vary from targeted criminal activity to accidental misconfiguration of settings.

Knowing how to respond to these cyber incidents is critically important, and having a plan in place that has been tested can greatly increase the likelihood of successfully overcoming an incident which reducing the impact on the organisation and its stakeholders.

This resource introduces incident response in the context of connected places projects and will help you in understanding the incident lifecycle and what to consider at each stage.

EXECUTIVE SUMMARY

What is this resource?

This resource has been produced to support local authorities with the challenge of responding to a cyber incident should it arise within their connected places projects.

How should I use it?

This resource is not an exhaustive set of actions and we do recommend you seek independent legal and technical advice, however it is designed to provide a useful starter before an incident arises.

The NCSC has detailed guidance on broader Incident Management should a cyber incident occur.

Who does this resource apply to?

The guidance set out here is particularly relevant to those who manage connected places projects and are responsible for setting and managing internal policy and processes.

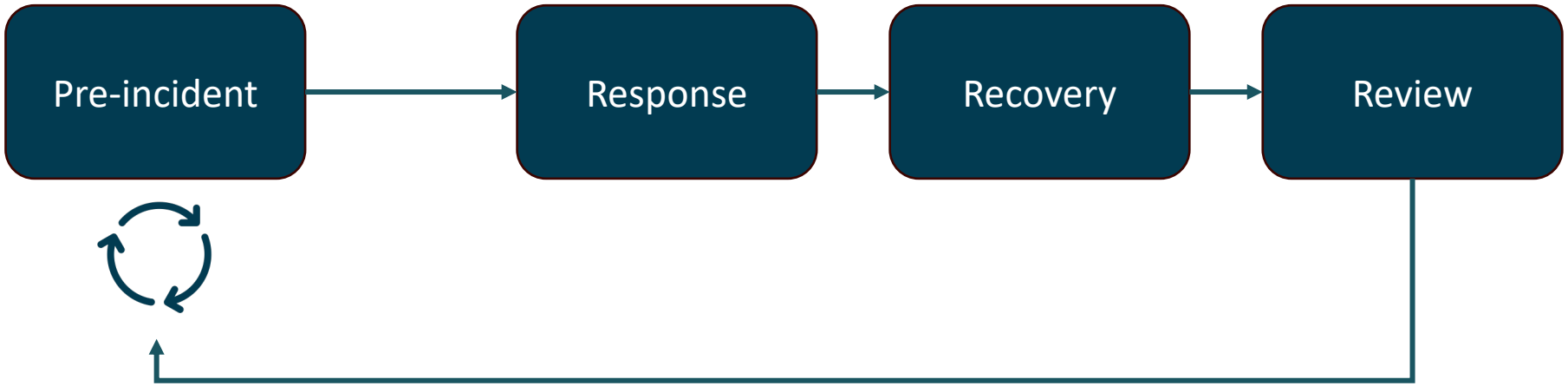
CONTENTS

INTRODUCTION

THE INCIDENT LIFECYCLE

Cyber incidents typically follow a lifecycle as shown here.

The speed at which an incident goes through this cycle depends on the scale and complexity of the incident and the response of the local authority. This can be from hours to months or even years.



Your local authority should have an existing cyber incident response plan covering the IT estate. It is critical that any connected places projects are aligned and integrated with this.

PRE-INCIDENT

INTRODUCTION

Before any incident even occurs there are several items of good practice that you should be conducting on a continual basis.

RISK ASSESSMENT

Ensure that there is a corporate system to govern and manage cybersecurity risk across all connected places projects.

See the Governance Resource for details

PLAN & TEST

Develop detailed plans for what happens if a cyber incident were to occur in a connected place project, regularly test these in realistic scenarios.

MONITORING

Continuously monitor for new cybersecurity threats and implement technical monitoring and logging for any anomalies or suspicious activity.

REPORTING

Provide simple means for internal and external people and groups to report cybersecurity concerns with your connected places project.

SUPPLY CHAINS

Monitor your supply chain for new and changing risks and work closely with them to manage these risks.

See the Procurement & Supply Chain Resource for details

REGULAR TESTING PLAN

Frequent realistic testing of your monitoring, response and recovery capabilities are highly recommended. Conducting these exercises will enable gaps to be identified, upon which policies and processes can be improved.

“Realistic” exercises in the context of a connected place ensures that real-world impacts of the response and recovery plan, upon the authority’s service delivery, are understood. Local authorities increasingly rely on sensing to enable data-driven operations the impact of denial of access to this data should be simulated with manual workaround processes defined and exercised.

Winter gritting operations increasingly rely on roadside temperature sensors

Road surface flooding prevention relies on gulley-based silt trap sensors

Social care increasingly relies on in-home air quality sensing to monitor patients

HOW TO KNOW WE HAVE AN INCIDENT

Continuous Monitoring

Much like corporate IT, connected places technologies can become compromised. To detect when an attack is taking place within connected places it is essential to implement real-time monitoring of network traffic, system logs, and behaviour analytics to detect anomalies or suspicious activities.

Supply Chain Vulnerability Management

Where services our outsourced to third parties it is vital to ensure that the third parties are contracted to be conducting the same level of monitoring internally as your organisation would if the service had been in sourced. In addition, suppliers should be contractually bound to report incidents to your local authority that supports your ability to meet regulatory requirements.

Vulnerability Disclosure

Members of the public, suppliers and security researchers may discover vulnerabilities or evidence of attacks to your systems. It is therefore recommended that local authorities implement a system that allows members of the public to identify the security point of contact to report such issues. The STRIDE resource within the Secure Connected Places Playbook discusses the “security.txt” / RFC9116 approach to providing a standardised means of contact.

Internal Reporting

The users of connected places systems are likely the ones who will see issues first. It is therefore essential that users are provided an interface to report issues. This might be through an internal help desk support function.

RESPONSE

NOTE: Detailed technical response guidance is published by the NCSC, available here.

TOUCHPOINTS

Various stakeholders will need to be communicated with to effectively manage the incident and ensure it has the minimal ongoing impact to the organisation.

IT teams within the local authority and **suppliers** should be made aware (if they are not already) so that the incident can be contained as quickly as possible and stop any spread to other systems.

It is recommended that **legal counsel** is sought to ensure the local authority conducts the incident in manner which is legal and protects its interests.

Where there is no internal capability, **specialist incident response companies** should be contacted as a matter of high priority – allowing the incident to be triaged, investigated and contained expediently. They may also be able to support with **Public Relations and Crisis Management,** drafting in clear communications with the public, members and staff.

Insurers should be contacted to ensure that all required measures are being taken.

The **National Cyber Security Centre** can be engaged to provide technical support where necessary. Similarly, the **National Crime Agency** may be contacted to report a cybercrime and may wish to investigate.

ICO must be notified within 72 hours of a breach "if a risk is likely to people's rights and freedoms"

Where there is a "a high risk to people's rights and freedoms", data subjects must be notified

COMMAND STRUCTURES

Depending on the severity of the breach a gold, silver, bronze command structure may be best employed to ensure situational awareness across the organisations and its partners

Bronze

OPERATIONAL

This team is primarily focused on day-to-day operations and the immediate response to a cyber incident.

The operational response involves activities such as detecting and containing the incident, isolating affected systems, and notifying relevant parties. It is about dealing with the incident at the ground level.

Silver

TACTICAL

Once the incident has been contained by the bronze team, the silver team takes a more detailed and coordinated approach to understand the incident's scope, impact, and root causes.

It includes conducting a thorough investigation, coordinating with various teams, and making decisions that address the immediate and intermediate-term goals of incident response.

Gold

STRATEGIC

This team provides executive leadership and makes high-level decisions that align with the organisation's overall business objectives and long-term goals.

It involves decisions related to resource allocation, legal considerations, public relations, and long-term improvements to the organisation's cybersecurity posture.

The gold team ensures that the incident response aligns with the broader strategic vision of the organisation.

It is important to identify and communicate the level of autonomy in decision making at these levels, to avoid delays to critical decisions. This is particularly important at the start of an incident where delays to action could prove to have significant consequences.

EVIDENCE CAPTURE

There is potential for a cyber incident to be criminal activity (although this is not always the case, for example, a piece of vulnerable software code is detected but has not been exploited).

Where a criminal activity is suspected to have taken place it is important to capture data and other material in a manner suitable for evidential use in the justice system.

This typically means that data as such as system logs are captured in their entirety and stored in a manner to remove any possibility of interference by others. This may include techniques such as:

- Storing data in a separate system that can only be accessed by extremely limited people
- All activity related to access to that data is securely logged with alerts to access
- That data cannot be edited or changed in any way
- Copies of that data are stored in multiple locations and systems in case of accidental (or deliberate) destruction
- Copies of that data are used for analysis, leaving the original untouched
- Physical evidence bags are used to keep hard drives and other devices, with appropriate controls and storage of these.

The technical standard for 'Digital Evidence Bags' published by ETSI is available here:
https://www.etsi.org/deliver/etsi_ts/103600_103699/103643/01.01.01_60/ts_103643v010101p.pdf

RACI MATRIX

Various parties will be required to input or be reported on the progress of the incident, this RACI matrix provides exemplar roles and responsibilities. It is not exhaustive, but it does represent a typical organisation.

	Responsible	Accountable	Consulted	Informed
Cabinet / Elected Members		x		
Governance Board (CPSSG)		x		
Legal			x	
Incident Manager	x			
Security Officer			x	
Technology Staff			x	

RECOVERY

RECOVERING TO AN OPERATIONAL STATE

Once the incident has been contained you may begin recovering. This will of course vary greatly depending on the severity of the incident and the plans and systems in place.

Suggested activities for recovery include:

- Restore data and systems from backups taken before the incident occurred
  - Ensure that these backups are not vulnerable to the same incident

- Adjust any processes or technology to ensure that any immediate or significant risks are appropriately managed, and that any change in process is documented and communicated appropriately. For example, you may immediately reset all passwords for accounts associated to the connected places project, this should be documented and communicated to all those impacted.

- Remove temporary measures if necessary and return to business-as-usual processes and structures.

- Conduct a new threat assessment for the connected places project, taking in to account any immediate changes made and what you know about the incident.

The STRIDE resource can be used to help you conduct a thorough threat assessment

REVIEW

LESSONS LEARNED

Conducting a lessons learned exercise following a cyber incident to a connected places project involves a structured approach to identify what went well, what didn't, and how to improve for future incidents. There are several key steps:

1. **Incident review:** Thoroughly review the incident, how it occurred, what was impacted, the response actions taken, and the timeline of events.

   Gather all relevant data, including logs and communications.

2. **Debriefing session:** Conduct a meeting to discuss the incident. Encourage open and honest communication. Focus on identifying what worked well and didn’t, without assigning blame.

   This must include a diverse range of stakeholders such as IT, legal, HR, PR, suppliers.

3. **Identify lessons learnt:** From the debrief session distil the key lessons learnt. Document these and validate with all relevant stakeholders.

4. **Develop action plans:** For each of the key lessons create a clear plan to address it, including who is responsible for it and the timeline for completion.

   As these are being implemented you should monitor and review their impacts.

5. **Document and share:** All of this should be clearly documented and shared within the local authority to improve cyber awareness. It may be shared wider, e.g. at cyber forums so that other organisations can learn from it too.

SUMMARY AND NEXT STEPS

INCIDENT RESPONSE: SUMMARY AND NEXT STEPS

1

KEY TAKE AWAYS

Good incident response starts before any incident even takes place.

Developing and testing response plans is critical to successfully dealing with an incident.

Your suppliers and a broad range of internal stakeholders should be included throughout.

Lessons should be learnt and actioned to continually improve.

2

QUESTIONS TO ASK

Do you have an incident plan specifically developed for your connected places projects?

Has this plan been tested with realistic scenarios?

Has this been communicated to the right people, including suppliers?

Does it align and integrate with broader authority incident plans?

3

NEXT STEPS

Review any existing plans, to identify any gaps and action these.

Engage with relevant internal and external stakeholders to validate and communicate the plan.

APPENDIX

GLOSSARY OF TERMS

Term/Acronym	Definition
Connected places	Connected places are a community that integrates information and communication technologies and Internet of Things devices to collect and analyse data to deliver new services to the built environment, and enhance the quality of living for citizens. A connected place will use a system of sensors, networks, and applications to collect data to improve its operation, including its transportation, buildings, utilities, environment, infrastructure, and public services.
Cyber incident	Any event that threatens the security, integrity, or availability of systems or components of systems. This can include information systems, networks, and data.
Cyber security	The practice of protecting computer systems from attack.
DSIT	Department for Science, Innovation and Technology.
ETSI	European Telecommunications Standards Institute.
ICO	Information Commissioners Office.
Log	A record that documents events, actions, and operations occurring within a computer system, network, or software application.
NCSC	National Cyber Security Centre.

THANK YOU

Department for Science, Innovation & Technology

In collaboration with

plexal DAINTTA Configured THINGS