



National Cyber
Security Centre
a part of GCHQ

Preparing for a highly disruptive cyber incident

How to prepare people, plans and processes so your organisation can respond and recover effectively



Contents

Introduction	2
About this guidance	3
1. Prepare your business continuity.....	5
1.1 Identify and prioritise critical services.....	6
1.2 Involve the wider community	6
1.3 Consider how to rebuild systems securely	7
1.4 Test and exercise plans.....	7
1.5 Cyber incident response (CIR).....	7
2. Prepare your people.....	8
2.1 Run regular practise exercises.....	9
2.2 Define roles and responsibilities.....	9
2.3 Plan alternative communication methods.....	10
2.4 Support staff welfare	10
2.5 Ensure sufficient skills and capacity	10
2.6 Plan for external support.....	11
3. Prepare your technical recovery capability	12
3.1 Securely store network and asset information.....	13
3.2 Maintain tested backups	13
3.3 Plan and test restoration processes.....	14
3.4 Document infrastructure dependencies.....	14
3.5 Enable logging and support observability	15
3.6 Secure cloud and operational technology environments.....	15
3.7 Arrange specialist incident response support	16
4. Prepare to make critical decisions	17
4.1 Consider taking pre-emptive containment action	18
4.2 Consider the risks of paying the ransom.....	18
4.3 Develop a communications strategy	19

Introduction

Although organisations should [take steps to prevent cyber attacks](#), there is no guarantee of avoiding a highly disruptive incident. Organisations that recover most effectively are those that prepare in advance – establishing the plans, people, technical capabilities and decision-making processes needed to operate through disruption and recover safely.

While much cyber security guidance focuses on preventing attacks, organisations must also be prepared for the possibility that an attacker succeeds despite those defences. Highly disruptive cyber incidents do not always result from a direct attack on your organisation. Disruption can also arise from cyber attacks affecting suppliers, managed service providers, technology providers or other organisations that your critical services depend upon. **Preparation for recovery is a core resilience capability, not an afterthought.**

As the NCSC CEO said in the 2026 RUSI Annual Security Lecture:

“The ability to absorb cyber attacks, contain their impact, sustain critical operations and recover quickly is no longer optional. It is a core competence for any digital organisation.”

Richard Horne, NCSC CEO

About this guidance

This guidance is for CEOs, CISOs, Boards and cyber professionals in large organisations. (Leaders of CNI organisations should also refer to our [guidance on planning for severe cyber threat](#) which sets out the additional, time-critical precautionary measures required in response to a significant step-change in the threat environment).

This guidance provides advice on how to prepare your organisation now – in advance of an attack – to:

- reduce its impact
- support informed decision-making under pressure
- enable faster recovery

Organisations should expect recovery to be delivered as a coordinated programme involving multiple workstreams across technical, operational and business functions. This is covered in depth in the NCSC's companion guidance on [recovering from a highly disruptive cyber attack](#).

What this guidance covers

There are 4 distinct areas of preparation:

1. **Business continuity:** prepare how your organisation will maintain and prioritise critical services during disruption, and plan for their structured recovery.
2. **People:** ensure your staff are ready to respond effectively, with clear roles, communication methods and the skills needed to operate under disruption.
3. **Technical recovery:** establish the systems, data, and processes required to securely restore technology and rebuild operations.
4. **Making critical decisions:** equip leaders with the authority, context, and principles they need to make timely, high-impact decisions.

Each of these areas is expanded in more detail in the sections throughout.

Why prepare?

During a disruptive cyber incident, you need to be able to make decisions quickly, communicate them effectively and coordinate a wide range of stakeholders and activities. When an incident is underway, you don't have time to think about what your response plan entails; you simply want to be confident it is ready to be used. Early planning also allows you to test and refine your response plans which helps ensure they are effective when they are deployed in earnest.

Many organisations document their response plan in a cyber incident 'playbook' or similar, setting out roles, responsibilities, escalation routes and recovery priorities.

1. Prepare your business continuity

You should understand which technology and business services are most important to your organisation, how long you can operate without them, and which systems support them. The following information should be captured in your [business continuity plan](#) (BCP).

Contents

- 1.1 [Identify and prioritise critical services](#)
- 1.2 [Involve the wider community](#)
- 1.3 [Consider how to build systems securely](#)
- 1.4 [Test exercise plan](#)
- 1.5 [Cyber incident response \(CIR\)](#)

1.1 Identify and prioritise critical services

During a disruptive cyber incident, full business as usual may not be possible. However, early preparation can help you maintain critical services at an acceptable level and restore them in a controlled way.

A clear **understanding of business-critical services** and their dependencies enables you to:

- identify feasible workarounds if technology is unavailable, and risk assess them
- prepare resources required to implement any workarounds
- prioritise systems for additional protection
- sequence system restoration effectively

Recovery should follow a **prioritised approach**, based on agreed business-critical services and the systems that support them.

1.2 Involve the wider community

Business continuity planning should involve:

- **stakeholders** from across the organisation – local teams often have the best understanding of how services operate in practice and what adjustments may be possible during disruption
- **customers/delivery partners** where critical services are delivered jointly or depend on shared processes – so that roles, priorities and workarounds can be agreed in advance
- **suppliers**, where critical services rely on them, including:
 - planning for abrupt loss of supplier services
 - understanding the resilience arrangements of key suppliers
 - considering the impact of supplier disruption on your operations
 - recognising that [attackers may target suppliers as a route into your organisation](#), or use supplier disruption to amplify operational impact

1.3 Consider how to rebuild systems securely

Your BCP should address how technology services will be restored if systems are compromised. Manual workarounds may provide short-term mitigation, but sustained recovery often requires organisations to establish trusted environments from which services can be securely restored. Planning and rehearsing this process in advance can help speed recovery and provide greater confidence that restored systems are secure and fit for purpose.

1.4 Test and exercise plans

Business continuity and recovery plans should be tested regularly and with a full exercise where possible, as many plans fail in practice. Testing and exercising can uncover issues that would have gone unnoticed until a real incident, at which point it is too late for changes and improvements.

Testing before a real incident occurs helps:

- identify gaps
- validate assumptions
- improve coordination

Exercising your plans in advance helps to expose weaknesses which may otherwise only become apparent during live response, when there is limited opportunity to adapt.

- **Tabletop exercises** can help validate governance, roles and decision-making.
- **Testing technical recovery procedures**, where possible, helps with understanding the practical complexities of restoration.

The NCSC provides a range of exercising support, including [Exercise in a Box](#) for practical, scenario-based exercises, and the [Cyber Incident Exercising \(CIE\) scheme](#) for more structured and advanced exercising.

1.5 Cyber incident response (CIR)

The NCSC recommends using [NCSC-assured Cyber Incident Response \(CIR\) providers](#) to support exercising and preparation activities, where appropriate.

2. Prepare your people

People are central to organisational resilience. During a disruptive cyber incident, technology and processes alone will not determine how well you respond. Your staff will need to adapt, make decisions in uncertain conditions, and find new ways to continue essential activities. Preparing them in advance helps ensure they can do this effectively.

Contents

- 2.1 [Run regular practise exercises](#)
- 2.2 [Define roles and responsibilities](#)
- 2.3 [Plan alternative communication methods](#)
- 2.4 [Support staff welfare](#)
- 2.5 [Ensure sufficient skills and capacity](#)
- 2.6 [Plan for external support](#)

2.1 Run regular practise exercises

It's useful for organisations to conduct regular [incident exercises](#) and simulations to help staff practise responding to disruption. These activities allow teams to test how they would operate if normal systems or processes were unavailable, and to experiment with alternative ways of working.

These exercises should involve both technical responders and wider organisational roles so that dependencies and decision-making processes can be tested.

2.2 Define roles and responsibilities

It's important to establish who is responsible for key activities during an incident, including:

- operational response
- technical recovery
- legal and regulatory
- decision-making
- communications

You should ensure that key decisions – for example, shutting down systems, invoking recovery plans, or communicating publicly – can still be made if senior leaders are unavailable.

Organisations should clearly define delegated decision-making authority so that high-priority operational decisions can be taken rapidly, including during out-of-hours periods.

The roles and responsibilities information should be kept up to date as staff change roles or leave the organisation.

You should also ensure responsibility is assigned for maintaining a clear record of decisions, actions and their rationale throughout an incident. Accurate records can support coordination, recovery activities, regulatory reporting, legal obligations and post-incident review.

2.3 Plan alternative communication methods

Disruptive cyber incidents may interfere with normal communication platforms such as corporate email or messaging services.

You should aim to [establish alternative and secure communication channels](#) that can be used to coordinate response activities if primary systems are unavailable or untrusted. It is also useful to maintain an offline copy of contact lists for key staff, suppliers and partners in case corporate directories are unavailable.

2.4 Support staff welfare

Responding to a disruptive cyber incident can involve long hours and sustained pressure, which can quickly lead to fatigue and burnout.

You should plan how you will [support staff during extended incidents](#), for example by:

- rotating responsibilities
- ensuring adequate rest periods
- providing additional support where needed

You should also make sure that employees outside the response team know what is expected of them if systems are unavailable – such as how to report issues, or whether to power down devices.

2.5 Ensure sufficient skills and capacity

A number of recovery activities can be highly resource intensive, for example:

- resetting large numbers of user credentials
- rebuilding systems
- reimaging devices
- issuing replacement laptops

You should assess whether you have the required skills and capacity to carry out these activities at scale and, if necessary, identify how you would secure additional resource during an incident. Critical response roles should never rely on a single individual.

2.6 Plan for external support

Many organisations will need assistance from external partners during a disruptive cyber incident.

You should identify the external organisations who may need to support recovery. These could include:

- IT providers
- cloud providers
- incident response partners

Establish relationships with them in advance where possible, and agree how you would communicate in the event of IT being unavailable during an incident.

3. Prepare your technical recovery capability

Response and recovery will need a skilled team with a strong understanding of the organisation's systems as well as the relevant data and accesses. The NCSC recommends undertaking the following activities to be prepared to recover and restore your systems.

Contents

- 3.1 [Securely store network and asset information](#)
- 3.2 [Maintain tested backups](#)
- 3.3 [Plan and test restoration process](#)
- 3.4 [Document infrastructure dependencies](#)
- 3.5 [Enable logging and support observability](#)
- 3.6 [Secure cloud and operational technology environments](#)
- 3.7 [Arrange specialist incident response support](#)

3.1 Securely store network and asset information

Ensure you maintain information about your networks and assets to support your organisation's response to complex or large-scale incidents.

Store your network and asset information in a secure location, separate from primary systems, to ensure it remains accessible if production systems are unavailable or offline, and to protect it from unauthorised access to prevent it being used by attackers

3.2 Maintain tested backups

Ensure you have [up-to-date, secure backups](#) as these are essential to an organisation's recovery process.

Backups should support the restoration of:

- data
- applications
- identity systems
- trust infrastructure
- configuration

You should do the following with your backups:

- have them tested regularly by third-party auditors
- protect them from unauthorised modification or deletion
- make them immutable where possible, as they are often a target of attackers who want to prevent a speedy recovery
- store them separately from primary systems

3.3 Plan and test restoration processes

When planning restoration, you should consider how systems will be brought back online and how data will be reconciled. Regularly test restoration processes to ensure they function as expected.

During an incident, organisations may well use manual processes or temporary workarounds that generate new data. Recovery plans should include how this newly-generated data will be validated and integrated with data restored from backups so that a single correct dataset is established.

When testing restoration processes, prioritise business-critical services, as restoring systems can take significant time.

3.4 Document infrastructure dependencies

Most business services rely on shared infrastructure such as identity services, networking, storage and cloud connectivity. Rebuilding complex infrastructure requires a good deal of planning and rehearsal.

To help with rebuilding, you should ensure you:

- maintain accurate network diagrams and asset inventories
- document system dependencies
- understand restart sequencing requirements
- store recovery documentation securely and separately from production systems

3.5 Enable logging and support observability

You should configure logging in systems in advance to help support investigation and recovery. Organisations should ensure they have observability across critical systems to detect malicious activity, understand the impact of an incident and support recovery decisions. The NCSC's blog on [observability and threat hunting](#), and [digital forensics](#) guidance provide further information.

Effective logging enables you to:

- understand how the incident occurred
- identify affected systems
- detect persistence mechanisms
- reduce the risk of repeat compromise

Organisations should ensure their logs are centrally collected, retained appropriately and accessible during recovery.

3.6 Secure cloud and operational technology environments

If you use **cloud services**, ensure they are securely configured, monitored and resilient so they can be accessed, controlled and safely restored during a disruptive incident. For further information, see the NCSC's guidance on [using software as a service securely](#) and [using a cloud platform securely](#).

Securing cloud services includes being able to:

- access administrative functions even if corporate networks are offline
- enforce strong authentication for cloud administration
- validate security posture before reconnecting systems
- plan the level of assurance required – as external connections may require certain levels of assurance before allowing the organisation to reconnect

Organisations with **Operational Technology (OT)** should ensure systems can be safely managed, recovered and restored during an incident, with full understanding of operational and regulatory impacts. This includes identifying where manual intervention may be required and testing restoration of OT systems to a known good state.

If your organisation has interconnections between IT and OT systems, you will need to ensure the recovery plans for both are aligned.

3.7 Arrange specialist incident response support

Most organisations do not retain in-house specialists who can respond to a disruptive cyber incident.

The NCSC recommends that all UK organisations, regardless of size, engage an [NCSC-assured Cyber Incident Response \(CIR\) provider](#) when responding to significant incidents. It's worth noting that your cyber insurance package may include CIR provision.

For more information on the importance of good technical preparation in advance of a cyber incident, see the NCSC Incident Management guidance on [effectively detecting, responding to and resolving cyber incidents](#).

You may wish to:

- identify and retain a CIR company in advance of an incident – conducting exercises with the team who would be on the ground during an incident helps preparation and can support faster mobilisation
- clarify suppliers' skills and experience as well as roles and responsibilities for each area of activity – for example, the CIR provider won't necessarily also rebuild IT systems

Ensure you store your cyber insurance details securely offline.

4. Prepare to make critical decisions

[Leaders must make high-impact decisions quickly](#) in the event of disruptive cyber incidents.

Organisations should identify in advance:

- who has the authority to make strategic decisions
- the organisation's risk appetite
- escalation thresholds
- legal and regulatory considerations

It may be useful to document your pre-agreed decision principles in your 'playbook' as this will help guide leaders when under the pressure of an unfolding incident. As outlined in the companion [guidance on responding to and recovering from a highly disruptive cyber incident](#), one of the first actions to take in the event of a disruptive cyber incident is to establish an **incident command structure** to enable rapid information exchange and decision making.

Contents

- 4.1 [Consider taking pre-emptive containment action](#)
- 4.2 [Consider the risk of playing the ransom](#)
- 4.3 [Develop a communications strategy](#)

4.1 Consider taking pre-emptive containment action

If an organisation becomes aware of the attack early enough, it may be possible to take action to halt the spread of the disruption, up to and including disconnecting systems. However, it should be noted that taking such actions may also cause disruption.

Planning ahead enables leaders to evaluate the potential impact of pre-emptive actions and to decide whether to pursue controlled disruption, rather than risk the uncontrolled disruption caused by an attacker. This decision will depend on the organisation's risk appetite.

Organisations responsible for essential services should consider **additional advance preparations** to enable rapid containment during periods of severe cyber threat. The NCSC's [guidance on responding to severe cyber attacks](#) highlights rehearsing in advance those actions which will quickly limit the impact of compromise. These may include:

- the ability to isolate systems
- operating critical services in a degraded or manual mode
- continuing essential functions while recovery is underway

4.2 Consider the risks of paying the ransom

The NCSC and UK law enforcement do not encourage, endorse or condone the payment of ransom demands.

Many disruptive cyber attacks are designed to maximise damage and pressure organisations into paying a ransom, but there are several risks with doing so. The NCSC's [Guidance for organisations considering payment in ransomware incidents](#) outlines these in detail. They include:

- there is no guarantee that you will get access to your data or computer, or that the stolen data will be deleted
- systems may remain compromised
- you may become a future target
- you may be funding criminal activity – [some criminals are sanctioned entities](#) and so you could even be breaking sanctions laws

In addition, even if an organisation is given the decryption key in exchange for the ransom, decryption of all machines can take weeks to complete. And there still remains the risk that the organisation hasn't fixed the underlying problems that permitted the attack in the first place. Well-prepared organisations are more likely to have alternative ways to recover that do not involve paying the ransom.

4.3 Develop a communications strategy

Large-scale attacks are likely to be noticed by individuals and organisations outside of your organisation. It would be useful to [develop a communications plan](#) to help you decide when and what information to share. This should include:

- defined roles and responsibilities
- pre-prepared messaging
- clear processes for notifying stakeholders
- alternative communication channels in case primary systems are unavailable

Keeping suppliers and customers appropriately informed can be important to maintain confidence and trust throughout the incident, as well as helping them manage the impact on their own businesses. This helps the resilience of your supply chain, and aids in returning to business as usual after the incident.

All communications should be:

- clear, accurate and timely
- tailored to different audiences
- maintaining consistent core messages, and avoiding speculation

This helps the resilience of your supply chain, and aids in returning to business as usual after the incident.

© Crown copyright 2026. Photographs and infographics may include material under licence from third parties and are not available for re-use. Text content is licenced for re-use under the Open Government Licence v3.0.
(<https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>)



NCSC.GOV.UK



@NCSC



@CYBERHQ



@CYBERHQ



National Cyber Security