



National Cyber
Security Centre
a part of GCHQ

Reducing the risk of highly disruptive cyber attacks

Practical steps to make it harder for attackers to gain access, spread through your systems and cause disruption



Contents

Introduction	2
About this guidance	3
1. Identifying critical systems, services and data	4
2. Reducing exposure to attack	5
2.1 Establishing baseline security practices	6
2.2 Reducing common entry points.....	6
2.2.1 Using stolen credentials.....	7
2.2.2 Finding an exploitable vulnerability.....	7
2.2.3 Targeting forgotten or unknown systems	7
2.3 Encouraging reporting and early detection.....	8
3. Limiting the impact of a successful compromise	9
3.1 Restrict access.....	10
3.2 Segment your network	10
3.3 Improve visibility and detection.....	10
3.4 Protect backups and administrative control.....	11
4. Building resilience into systems.....	12
5. Detecting and responding to attacks quickly.....	13

Introduction

Highly disruptive cyber attacks, such as ransomware, can prevent organisations from operating normally by denying access to systems, disrupting essential services, and causing significant financial and operational damage. In ransomware attacks, attackers seek to maximise disruption in order to increase pressure on victims to pay a ransom.

While this guidance focuses on reducing the risk of such attacks, some cyber risk will always remain. To minimise the impact of attacks that are successful, organisations must also [prepare for disruptive cyber incidents](#).

About this guidance

This guidance is intended for senior decision makers and those responsible for organisational resilience. It provides a framework for identifying and prioritising investment in cyber security fundamentals, and taking action early, to reduce the likelihood and impact of highly disruptive cyber attacks.

The guidance is especially useful for organisations seeking assurance that appropriate measures are in place to protect critical services and operational delivery. Organisations already following [Cyber Essentials](#) or another recognised cyber security framework, are likely to find that many of the measures described here are already reflected in their existing security activities.

Understanding the path to disruption

It's useful to note here that there are typically 2 distinct stages of attacker behaviour in highly disruptive cyber attacks:

- 1. Initial access where attackers gain a foothold in the organisation's environment.**
- 2. Expansion and disruption where attackers move through the environment, targeting critical systems and data to maximise operational impact.**

Understanding these stages helps organisations focus their defences where they are most effective.

This guidance is organised into 5 sections that help organisations strengthen their resilience. These are not sequential steps, but complementary capabilities that work together to reduce the risk and impact of highly disruptive cyber attacks:

- [1. Identifying critical systems, services and data](#)
- [2. Reducing exposure to attack](#)
- [3. Limiting the impact of a successful compromise](#)
- [4. Building resilience into systems](#)
- [5. Detecting and responding to attacks quickly](#)

Sections 2 and 3 focus on preventing initial access and restricting attacker movement, while sections 1, 4 and 5 support these activities by helping organisations identify critical assets, design resilient systems and improve detection.

1. Identifying critical systems, services and data

You cannot defend your systems effectively without understanding what you have. Gaps in visibility can become entry points for attackers or allow them to operate undetected. You should [build a clear picture of your systems, services and data](#) to identify where weaknesses may exist, allowing you to respond more quickly to emerging risks.

Attackers often focus on specific high-value targets that allow them to maximise disruption.

These typically include:

- high privilege accounts
- identity and access management systems such as Active Directory
- backup systems
- systems underpinning essential functions

2. Reducing exposure to attack

A cyber attack can start from many different entry points. Reducing your attack surface makes it harder for attackers to gain an initial foothold. This section outlines measures to achieve this.

Contents

- 2.1** [Establishing baseline security practices](#)
- 2.2** [Reducing common entry points](#)
- 2.2.1** [Using stolen credentials](#)
- 2.2.2** [Finding an exploitable vulnerability](#)
- 2.2.3** [Targeting forgotten or unknown vulnerabilities](#)
- 2.3** [Encouraging reporting and early detection](#)

2.1 Establishing baseline security practices

A strong foundation starts with applying baseline cyber security practices. Frameworks such as [Cyber Essentials](#) or the [Cyber Assessment Framework](#) (CAF) provide a structured way of reducing common risks of attack, such as:

- securing configurations
- managing access
- keeping systems up to date

2.2 Reducing common entry points

Cyber security teams should ensure that common attack routes are being addressed. 2.2.1–2.2.3 show some of the common techniques attackers use to gain entry to a network, and the relevant NCSC guidance to help prevent or mitigate them.

2.2.1 Using stolen credentials

Common ways an attacker can gain access to your network

Attackers often use compromised usernames and passwords to gain access to systems.

Relevant NCSC guidance:

- Enforce strong [password policies](#).
- Implement [strong methods of multi-factor authentication \(MFA\)](#).
- [Make passkeys available as an option](#) where possible.
- Improve your organisation's [resilience against phishing attacks](#).

2.2.2 Finding an exploitable vulnerability

Common ways an attacker can gain access to your network

Attackers gain unauthorised access by exploiting vulnerabilities or insecurely configured services that are exposed to the internet.

Relevant NCSC guidance

- Establish a [vulnerability management process](#) to keep your systems protected throughout their lifecycle.
- [Securely configure internet-facing systems](#) and disable unnecessary services
- [Keep all applications up to date](#).
- If using bespoke apps, [establish controls in the application development phase](#).

2.2.3 Targeting forgotten or unknown systems

Common ways an attacker can gain access to your network

Attackers can gain entry via systems you aren't monitoring or even aware of.

Relevant NCSC guidance:

- Use [attack surface management tools](#) to help you discover and manage unknown parts of your attack surface.
- Reduce the use of shadow IT [through improving access to managed options](#).

2.3 Encouraging reporting and early detection

Early reporting increases your chances of identifying and stopping attacks before they escalate. People across the organisation are likely to be the first to notice signs of an attack, so you should ensure they can report issues easily.

To support this, you should:

- provide clear and simple reporting mechanisms
- [promote a culture](#) where reporting of suspicious activity and mistakes is both expected and supported

3. Limiting the impact of a successful compromise

Even well-protected organisations may experience a cyber attack. When this happens, the organisation's ability to limit attacker movement becomes critical. As highlighted in the NCSC's [guidance on preventing lateral movement](#), organisations should assume an attacker may already have a foothold. They should focus on detecting attacker activity and limiting the damage it can cause.

After gaining access to a network, attackers typically try to:

- increase their level of access (privilege escalation)
- move between systems (lateral movement)
- locate critical systems and valuable data

Slowing this activity using multiple layers of protection and mitigation – often referred to as defence-in-depth – gives organisations more time to detect and respond, and reduces the overall impact of the attack. The remainder of this section outlines defence-in-depth techniques. These controls should be used across your networks to limit an attacker's opportunities. You should pay particular attention to your critical assets and other attractive targets.

Contents

- 3.1** [Restrict access](#)
- 3.2** [Segment your network](#)
- 3.3** [Improve visibility and detection](#)
- 3.4** [Protect backup and administrative controls](#)

3.1 Restrict access

Controlling access is one of the most effective ways to limit what attackers can do. Applying the [principle of least privilege](#) ensures that users and systems only have access to what they need at the time they need it. This reduces opportunities for attackers to escalate privileges or move more widely. In practice this means you should:

- grant access based on role and necessity
- review and remove unnecessary permissions
- enforce access policies before allowing access, for example through [Zero Trust Network Access \(ZTNA\)](#)

3.2 Segment your network

[Network segmentation](#) limits how far an attacker can move within an organisation's environment. Without segmentation, a compromise in one area can quickly spread to others. By dividing your network into controlled segments, you're able to:

- restrict access to sensitive systems and data
- contain incidents more effectively

Network segmentation is most effective when it is built into system design, as outlined in section 4.

3.3 Improve visibility and detection

The earlier an attack is identified, the more effectively an organisation can respond and limit disruption. [Organisations should develop strong observability across their systems, services and networks](#), giving them the information needed to detect unusual activity, investigate incidents and understand their cyber risk.

To support this, organisations should:

- establish appropriate monitoring across critical systems and services
- develop the capability to identify and investigate anomalies and potential threats
- ensure security teams can respond quickly to signs of compromise
- continuously improve detection capabilities as technologies and threats evolve

3.4 Protect backups and administrative control

Backups and administrative access accounts are frequent targets in disruptive attacks. If attackers can compromise them, they can significantly increase the scale of damage – such as deletion or destruction of data – or gain broader access to more data.

To reduce this risk, you should:

- [secure and isolate backups from the main network](#)
- regularly test recovery processes
- [apply additional controls to administrative access](#)
- [limit, review and monitor access to critical systems](#)

4. Building resilience into systems

Security and resilience are most effective when they are [built into systems from the outset](#). Retrofitting controls later is often more complex and less effective. Where organisations rely on legacy systems, these principles can be used to guide upgrades, integrations and other changes, helping improve security and resilience over time.

When designing or updating existing systems, organisations should consider how they will:

- prevent unauthorised access
- limit attacker movement
- support detection and response

[Zero trust principles](#) can help reduce opportunities for unauthorised access and limit attacker movement. As explained in the NCSC's [Zero Trust Network Access guidance](#), this means verifying access continuously, rather than assuming trust based on network location.

You can also improve security by:

- using dedicated and hardened environments for administrative tasks, for example: following NCSC guidance on
- [privileged access workstations](#)
- reducing unnecessary system complexity
- limiting dependencies between critical systems

For organisations using Operational Technology (OT), it's important to carefully manage connectivity between IT and OT environments, ensuring that interactions are tightly controlled and aligned to the NCSC's [cross-domain principles](#) for securely managing data flows between systems of differing trust.

To this end, you should:

- secure and monitor connections between networks
- restrict access to essential interactions only
- design systems to limit the impact of compromise

5. Detecting and responding to attacks quickly

In addition to prevention and containment, you should use services that help detect and disrupt malicious activity.

To improve detection, the NCSC recommends the following services:

- Protective DNS (PDNS) services which prevent systems from connecting to known malicious domains. This can stop malware communicating with attackers and reduce the impact of an incident. The NCSC provides a [PDNS service](#) for the public sector, and [commercial PDNS services](#) are available for private sector organisations.
- The NCSC's free [Early Warning service](#) which provides alerts based on trusted data sources to help identify threats affecting your network

© 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