THE CYBER RESILIENCE CENTRE NETWORK

Preparing for a Cyber Incident

Tools and Tips for the Care Sector

Delivered on behalf of the CRC Network by:
Paul Lopez, *Director*
Sapphire Little, *Business Development Manager*
Lucy Dover, *Business Development Assistant*

WWW.ECRCENTRE.CO.UK

Delivered in partnership with

CARE ENGLAND
The voice of care

The Care Provider ALLIANCE

Agenda

Why cyber matters in care

Incident Response planning

How to access support and get in touch

Assess your current cyber resilience

Strengthen your defences with free tools and resources

THE CYBER RESILIENCE CENTRE NETWORK

Why cyber matters in care

Why cyber matters in Care

Care providers hold sensitive personal and medical data:

Think about everything you hold on your residents or service users:

- Medication records
- Financial details
- Next of kin
- Mental health history
- Care plans

To a criminal, that information is valuable. It can be sold, held to ransom, or used to commit fraud. You may not think of yourself as a target, but the data you hold makes you one.

NHS and care supply chains are increasingly interconnected

Many care providers now share data with NHS systems, use digital care management platforms, or receive referrals electronically.

That connectivity is brilliant for joined-up care - but it also means an attack on one part of the chain can affect others.

You don't have to be the primary target to be caught up in an incident.

Staff are time-pressured and often targeted through phishing

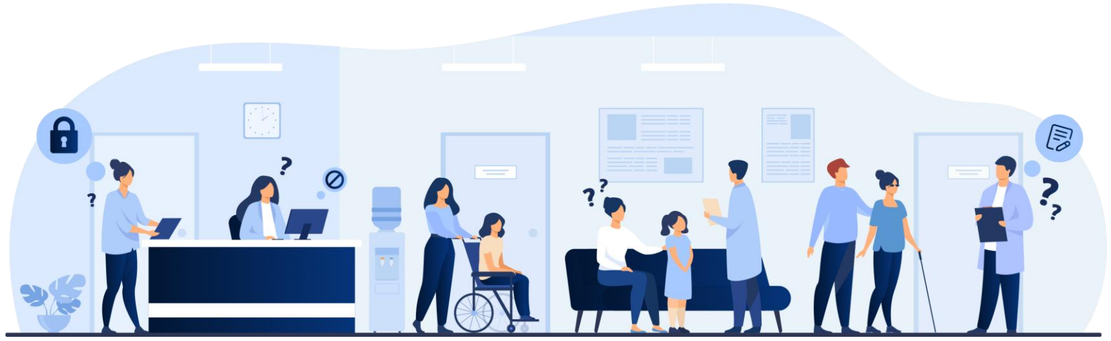
A night shift carer rushing between calls, a manager dealing with a staffing crisis - these are exactly the moments criminals exploit.

A convincing email pretending to be from the CQC, HMRC, or even a colleague asking for a password reset takes seconds to fall for. **It's not about being careless, it's about being human under pressure**.

The real-world impact

What happens when a cyber incident hits a care provider?

A cyber incident isn't just an IT problem.



Service users at risk

If **systems go down**, who is responsible for checking the medication round? Who can access care plans or DNR records?

It directly **affects the safety and dignity** of the people in your care.

Staff locked out

Potential loss of access to rotas, care records, and contact details.

Staff are left relying on memory and paper which is not just inconvenient, but a genuine safety risk.

Medication and care plans inaccessible

With **no access to medication and records**, staff may be left to face impossible judgement calls.

Care plans for complex needs may be completely unavailable.

Safeguarding disrupted

Logs inaccessible, communication breaks down, **ongoing concerns left without oversight.**

A cyber incident can knock out **documentation, communication** and **accountability** at once.

Consequences that may follow

Reputational, financial, and regulatory consequences

The **ICO (Information Commissioner's Office)** may need to be notified within 72 hours if personal data was involved - **missing that deadline can mean fines**

The **CQC (Care Quality Commission)** expects to be informed if the safety or continuity of care was affected - **it can impact your inspection rating**

Average cost to a care provider: £9,528 *(DHSC, 2025)* Costs include IT recovery, staff overtime, legal advice, and potential fines - **significant for any provider operating on tight margins**

Families will want answers, and that conversation is very hard without a prepared response

THE CYBER RESILIENCE CENTRE NETWORK

Assess your current cyber resilience

NCSC My Cyber Action Toolkit

What is it?

- Free tool from the National Cyber Security Centre – the UK's governing body for cyber
- Designed to helps organisations like yours understand their current cyber security posture
- Generates a personalised action plan based on your answers
- No technical knowledge required
- Takes around 30 minutes to complete

Where to find it: ncsc.gov.uk > Small organisations > My Cyber Action Toolkit

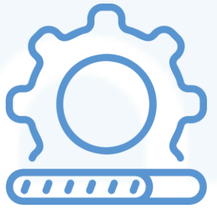
What the Toolkit Covers

The toolkit assesses you across

5 Key Areas

Backing up data:
Are your records protected if systems fail?

Protecting against malware:
Are devices and systems defended?



Keeping devices up to date:
Are software and systems patched?

Using strong passwords & MFA:
Are accounts properly secured?

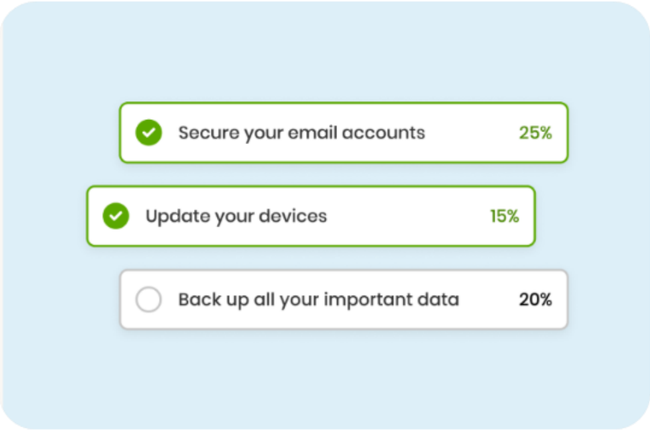
Avoiding phishing attacks:
Can your team recognise suspicious messages?

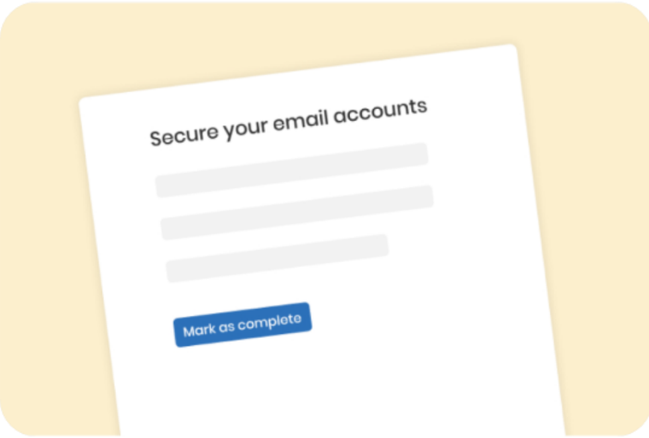
These map to NCSC's Cyber Essentials framework

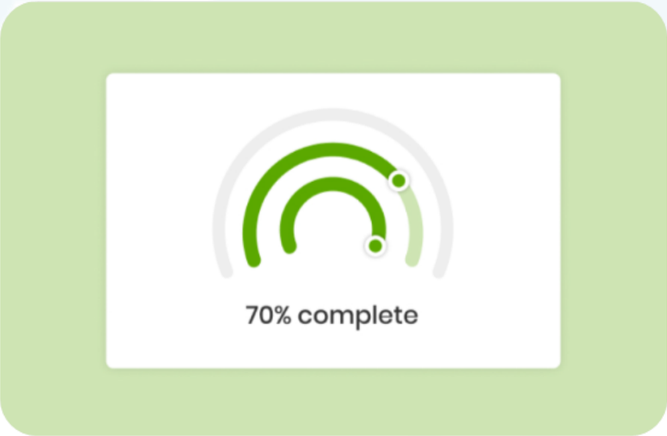
How to Use the Toolkit in Your Organisation

Practical steps:

1. **Assign a lead** (doesn't need to be IT - a manager or compliance lead works)
2. **Work through the questions as a team** if possible
3. Use the **output as your starting point,** not a pass/fail grade
4. **Share results** with your governance or leadership team
5. **Revisit** every 6–12 months or after a significant change







THE CYBER RESILIENCE CENTRE NETWORK

Incident Response planning

What is an Incident Response Plan

A written, practical plan that tells your team:

What counts as a cyber incident
From being locked out of your systems, to a staff member clicking a suspicious link, to a device with resident information going missing

Who is responsible for what
Naming actual people, not just job titles, so everyone knows exactly what to do at 7am on a Sunday without having to ask

How to contain and recover
Disconnect the affected device, switch to paper records, don't pay any ransom before speaking to IT, and restore from backups

Who to call and in what order
IT support, Report Fraud, your insurer, ICO, CQC - written down in advance so no one is searching for numbers in a panic

Key message: You don't need a complex document - a simple, clear, one-page plan is better than nothing.

The Five Stages of Incident Response

1 IDENTIFY

Spot that something is wrong, whether that's a ransom message on screen, a staff member who clicked a suspicious link, or systems that suddenly stop working

2 CONTAIN

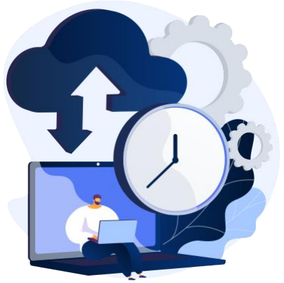
Stop it spreading by disconnecting affected devices from the internet and your network, and switching to paper records for care delivery in the meantime

3 ASSESS

Work out what's been affected, which data may have been accessed, and whether resident safety or care continuity has been impacted

4 RECOVER

Restore your systems and data from backups, check everything is working correctly, and only reconnect devices once you're sure they're clean



5 REVIEW

Once the dust settles, look at what happened, how your team responded, and what you'd do differently — then update your plan accordingly

Reporting Obligations for Care Providers

You may need to report to:

Internal contacts

e.g. Senior Leadership Team / IT Support Provider - **inform them immediately so decisions can be made quickly** and the right people are in the loop

CQC (Care Quality Commission)

If the incident **affects the safety or continuity of care, they expect to be informed** and it can impact your inspection rating

NCSC

For significant incidents: **report.ncsc.gov.uk**

ICO (Information Commissioner's Office)

If **personal data** has been breached, you may have just **72 hours to report it** or risk a fine

Report Fraud / Police

To report the crime: **0300 123 2040** or **reportfraud.police.uk**

Your cyber insurance provider

Call them before you spend anything on recovery

Build these contacts into your plan now so if the worst happens, your team knows exactly who to call

Cyber in your Business Continuity Plan

Cyber incidents are a business continuity issue, not just an IT issue

Things to consider:

? Do your BCP and fire/flood plans include a "cyber scenario"?

? What's your fallback if your care management software is unavailable?

? Do you have paper-based backups of critical care records?

? Can staff communicate and work without your usual systems?

NCSC recommendation: Test your plan at least once a year – Exercise in a Box is free and designed for this

THE CYBER RESILIENCE CENTRE NETWORK

Strengthen your defences with free tools

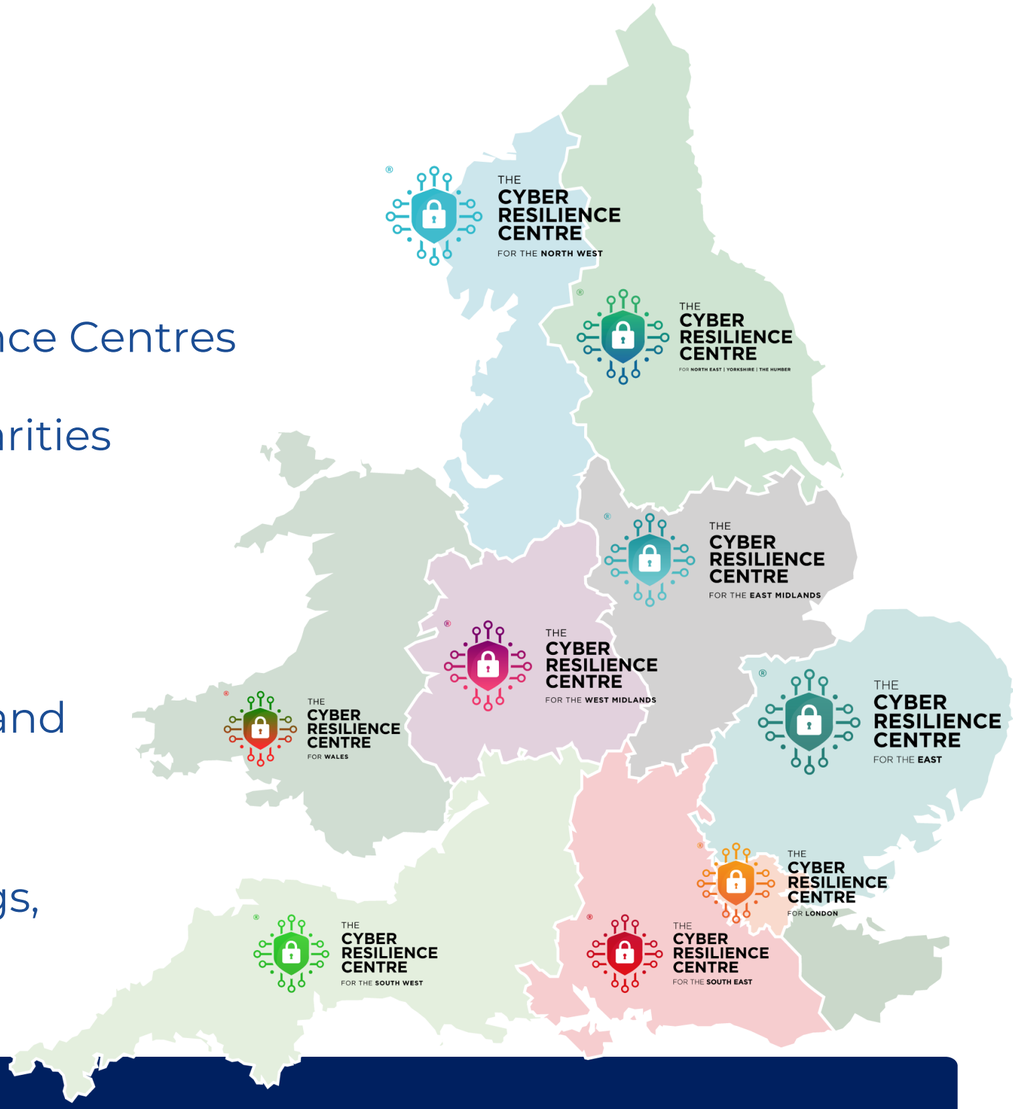
The CRC Network

Who we are

- **Police-led, government-funded** network of Cyber Resilience Centres
- **Working to support** small and medium organisations, charities and the third sector

How we can support your organisation

- **We offer a wide range of fully funded, interactive tools** and training resources to help build cyber awareness
- **These can be incorporated into** inductions, team meetings, and refresher courses



Our aim: to increase the cyber resilience of small and medium businesses, charities and the third sector

THE CYBER RESILIENCE CENTRE NETWORK

Police-led, **Business**-focused

CRC Membership

Provides members with:

- **Regular newsletters and cyber awareness updates** featuring the latest guidance
- **Regional and national threat alerts** around the latest scams
- **Signposting to free tools and resources** from local policing and the NCSC
- **Access to a wide range of Cyber Security Services** via our Cyber PATH programme including training, vulnerability assessments, Microsoft 365 reviews etc

Scan the QR code to sign up

There are 9 regional Cyber Resilience Centre's across England and Wales

Unlocking the benefits of CyberPATH for your organisation

CYBER PATH
POLICE & ACADEMIA TALENT HORIZONS

- CyberPATH is an **elite talent pipeline**, recruiting students from **top UK universities.**
- Students are trained to deliver a range of **cyber services,** which are available to SMEs at **no cost** to their organisation.
- CyberPATH provides SMEs with **expert cybersecurity solutions,** simultaneously providing **hands-on experience** for the **future cyber workforce.**

10 Fully funded Cyber PATH Services Available

CYBER PATH
POLICE & ACADEMIA TALENT HORIZONS

Security Awareness Training

Staff training for those with little or no cyber security or technical knowledge

First Step Web Assessment

Provides you with an initial assessment of your website to highlight its most pressing vulnerabilities

Internal Vulnerability Assessment

Scan and review your internal networks and systems looking for vulnerabilities

Microsoft 365 Service

Reviews your Microsoft 365 configuration to identify any flaws in your organisation's set up.

Internet Discovery Service

Comprehensive review of publicly available information about any potential or existing employee.

Cyber Business Continuity Review

A thorough review of your business continuity plan and overall resilience to cyber attacks

Police Cyber Alarm

POLICE CYBERALARM

What is it?

- **Free service from** the Police Digital Security Centre
- **Acts like a "CCTV camera"** Monitors your internet traffic for signs of malicious activity
- **Sends you alerts if suspicious activity is detected and provide regular reports** of suspected malicious activity, enabling organisations to minimise their vulnerabilities.
- **Designed to protect** personal data, trade secrets and intellectual property, and helps to build a national picture of new and emerging cyber threats
- **Does not interfere** with normal network operations.

Who should sign up: Any care provider with a broadband connection

Where: policealarmsystem.co.uk

NCSC Exercise in a Box

Practise your response before an incident happens

Free online tool from the National Cyber Security Centre to help organisations rehearse their response to cyber attacks.

→ **No technical expertise needed** to facilitate

→ Takes **1–2 hours** to run

→ **Realistic** cyber incident scenarios you can run as a **team exercise**

→ **Scenarios include:**

- Ransomware
- Phishing
- Supply chain
- Risk management
- Passwords
- Vulnerabilities

Where: exerciseinabox.ncsc.gov.uk

THE CYBER RESILIENCE CENTRE NETWORK

Next steps

Your next steps

Register for our free support

Gain access to regular cyber-awareness updates, and a wide range of fully funded tools and resources designed to strengthen your organisation's cyber resilience

Book a 1-to-1 session

We'll check in, answer any questions, and explore which of our fully funded cyber resilience services are best suited to your organisation's needs

Complete the NCSC My Cyber Action toolkit

Get a service booked in for your organisation, and receive ongoing support from The CRC Network to help build long-term cyber resilience

Draft or review your incident response plan

Use the five stages covered in this session as your starting point - identify, contain, assess, recover, review

THE CYBER RESILIENCE CENTRE NETWORK

Police-led, **Business**-focused

Book a 1-to-1 session with us today

Discuss anything we've covered in more detail and take your first step towards cyber resilience

Delivered in partnership with

CARE ENGLAND
The voice of care

The Care Provider ALLIANCE