Departure
Sir Julian Hartley steps down as CQC chief executive

Workforce
Adult social care's economic contribution grows

Welltower
Investor strikes Barchester and HC-One deals

NOVEMBER 2025 | VOLUME 33 | ISSUE 7

CM CareMarkets

Independent. Intelligent. Insightful.

Getting started

The digital journey

LaingBuisson
INTELLIGENCE + INSIGHT

Cyber threats in care homes are no longer hypothetical. **Helen Tringham**, partner at Mills & Reeve, explores how the care sector's growing reliance on digital systems has made it a prime target for cyber-attacks

Reducing **your risk**

Over the past decade, the health and care sector has faced a growing number of cyber-attacks. High-profile incidents such as the 2017 Wannacry ransomware attack and the 2024 Synnovis breach, which exposed sensitive NHS data, have caused widespread disruption, cancelled treatments, and led to rectification costs running into hundreds of millions of pounds. In 2025, the Information Commissioner's Office (ICO) fined Advanced Computer Software Group Ltd £3.1m after a ransomware attack compromised the data of nearly 80,000 people.

The sector's increasing reliance on digital systems, especially for health and incident records, means that care homes are particularly vulnerable due to the sensitive nature of the data they hold.

Why cybersecurity matters

Cyber incidents in care settings can have severe consequences. A cyber-attack can bring essential systems to a standstill, making it difficult or impossible to access care records, medication charts, or incident logs. This can lead to delays in administering medication, missed appointments, and an inability to monitor residents' health effectively. In some cases, care homes may have to revert to paper-based systems, which are slower and more prone to error. The resulting operational disruption can compromise the quality and continuity of care, potentially putting residents' health and wellbeing at risk.

Care homes hold highly sensitive information about residents, including medical histories, care plans, and family and personal details, as well as staff records. A data breach can result in this confidential information being accessed, stolen, or published by unauthorised parties. This violates the privacy of residents and staff, and can lead to identity theft, fraud, or targeted scams. The emotional impact on those affected can be significant, eroding trust in the care provider.

The UK's data protection laws require care homes to safeguard personal data. Failure to do so can result in substantial fines from regulators such as the ICO. Beyond financial penalties, a cyber incident can severely damage a care home's reputation. News of a breach may deter prospective residents and their families, undermine relationships with commissioners and partners, and lead to increased scrutiny from regulators. Rebuilding trust after a cyber incident can be a long and challenging process.

Key risks for care homes

Most incidents stem from human error. Key risks include:

- **Phishing attacks:** Scam emails that appear genuine but contain malicious links, potentially installing harmful software.
- **Accidental data breaches:** For example, sending information to the wrong recipient or leaving care plans in public areas.
- **Deliberate cyber-attacks:** External attempts to gain unauthorised access, often following the compromise of credentials via a phishing event.

UK data protection law requires care homes to implement appropriate technical and organisational measures to keep systems secure. We share below some practical strategies to help you meet these obligations:

1 Implement robust cybersecurity measures

It is crucial to ensure your care home has strong cybersecurity protocols in place.

- Use firewalls, antivirus software, multi-factor authentication (MFA), and intrusion detection systems.
- Keep all software up to date and conduct regular security audits to identify and address vulnerabilities.
- Ensure that all devices and systems are protected, including those used by staff working remotely.

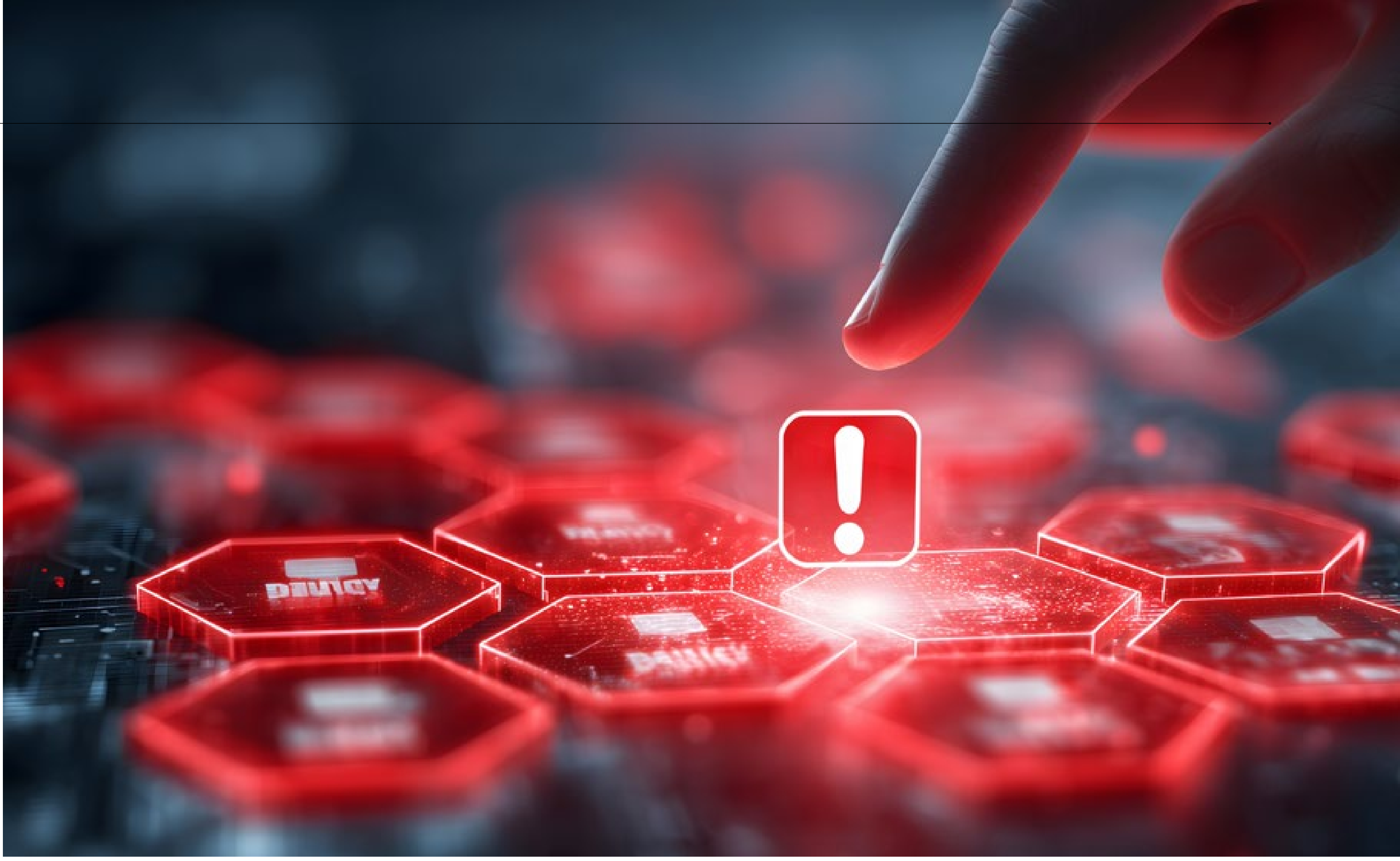
2 Train staff on cybersecurity best practice

Your staff are your first line of defence against cyber-attacks. It is important for staff to understand what a cyber-attack looks like and who to report it to, so that swift action can be taken.

- Provide regular training and testing on recognising phishing emails, using strong passwords, and secure data handling.
- Foster a culture of cyber awareness – staff should know how to spot a cyber-attack and who to report it to.
- Include business continuity steps in training, so staff know what to do if systems are compromised.

3 Regularly back up data

- Back up all critical data frequently and store backups securely, both on-site and off-site.



- Test backups regularly to ensure that systems can be restored in practice.
- Consider the sensitivity of different types of data and apply appropriate security measures. The ICO expects that more sensitive or potentially damaging data will be treated with a higher level of care.
- Weigh the pros and cons of cloud-based versus physical backups. Cloud-based backups remain popular due to their scalability and accessibility, but they carry risk of security concerns and overdependence on cloud providers. A hybrid approach can provide resilience and flexibility.

4 Develop a comprehensive incident response plan (IRP)

An IRP sets out what to do during and after a cyber incident. If the IRP is well thought out and tested against hypothetical scenarios, it will minimise delay and operational disruption in a real-life event.

- An IRP should include:
  - Identification of critical assets and likely threats
  - Defined roles and responsibilities for response team members
  - Procedures for detecting, containing, and eradicating threats
  - Steps for recovering systems and restoring operations
  - Post-incident reviews to improve future responses
- Test your IRP with hypothetical scenarios to ensure it works in practice and minimises disruption.

5 Understand and meet your reporting obligations

Understanding your legal obligations around data breaches is essential for every care home provider. Prompt and accurate reporting not only ensures compliance with data protection laws but also helps to protect the rights and wellbeing of residents and staff.

- If a breach affects personal data, you may need to report it to the ICO within 72 hours.
- Remember that a lack of access to personal data (not just unauthorised access) can be a reportable breach if it risks individuals' rights and freedoms.
- Failing to report can result in significant fines and reputational harm.
- Consider investing in cyber insurance

6 Cyber insurance can help manage the financial impact of incidents and provide access to expert support

- When choosing a policy, check for:
  - Coverage for data breaches, ransomware, and business interruption
  - Inclusion of legal, forensic, and public relations support
  - Clear policy exclusions and limitations
- Cyber insurance should complement, not replace, robust cybersecurity measures. Standalone cyber policies usually offer broader coverage and higher protection than general business insurance.

Final thoughts

Cybersecurity is a critical issue for care home providers, given the sensitivity of the data involved and the vulnerability of service users.

By taking proactive steps – implementing strong security measures, training staff, backing up data, planning for incidents, and considering insurance – you can significantly reduce your risk.