Quality Care Group

Cyber Risk in Care

An executive guide for care providers

hello@qcaregroup.co.uk | www.qcaregroup.co.uk

Protecting what matters most

hello@qcaregroup.co.uk | www.qcaregroup.co.uk

Care providers face a growing range of risks, from safeguarding concerns and workforce challenges to increasing regulatory scrutiny.

Alongside these challenges sits a threat that has grown rapidly over the last decade: cyber crime.

For many organisations, cyber risk is no longer simply an IT issue. It is a business continuity, governance and resident safety issue that requires attention at leadership level.

Why Cyber Risk matters to care providers

hello@qcaregroup.co.uk | www.qcaregroup.co.uk

The care sector holds some of the most sensitive information in the UK economy.

Care providers routinely manage:

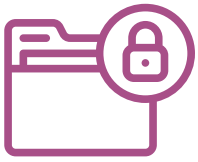
Resident health records

Financial data

Personal information

Employee information

Medication records



Safeguarding documentation

At the same time, care businesses depend on systems that must remain available around the clock.

This combination makes the sector an attractive target for cyber criminals.

The threat landscape has changed

Historically, care organisations focused heavily on physical risks such as fire, theft and property damage.

These remain important.

However, cyber attacks are increasing in frequency, sophistication and financial impact.

Unlike many traditional risks, cyber incidents can affect multiple sites simultaneously and cause disruption within minutes.

For care providers, the consequences can extend far beyond financial loss.

The real world impact of a cyber incident

A successful cyber attack can create challenges across every area of a care business.

Operational Disruption

Critical systems may become unavailable without warning, preventing access to care records, communication systems and operational data.

Resident Safety

When information systems become inaccessible, staff may need to rely on manual processes, increasing pressure during an already stressful situation.

Regulatory Consequences

Data breaches can trigger investigations from the Information Commissioner's Office and wider scrutiny around governance, security and data protection.

Financial Losses

Recovery costs, legal expenses, business interruption and fraud losses can quickly escalate.

Reputational Damage

Trust is fundamental within the care sector. A significant cyber incident can affect confidence among residents, families, staff and commissioners.

Common cyber threats facing care providers

Phishing Attacks

Fraudulent emails designed to trick staff into revealing information, clicking malicious links or downloading harmful software.

Ransomware

Criminals encrypt business systems and demand payment for their release.

Business Email Compromise

Attackers impersonate trusted suppliers or colleagues to authorise fraudulent payments.

Data Breaches

Unauthorised access to sensitive resident, employee or financial information.

Third Party Risks

Vulnerabilities within suppliers, software providers or outsourced services that can expose your organisation to attack.

Building cyber resilience

hello@qcaregroup.co.uk | www.qcaregroup.co.uk

Effective cyber security is not about eliminating risk entirely.

It is about reducing the likelihood of an incident and improving your ability to respond when one occurs.

Practical measures include:

- ✅ **Multi-factor authentication**
- ✅ **Strong password policies**
- ✅ **Regular software updates**
- ✅ **Tested data backups**
- ✅ **Cyber awareness training**
- ✅ **Incident response planning**
- ✅ **Supplier due diligence**

Organisations that adopt these measures are often better positioned to prevent incidents and recover more quickly when they occur.

A real world example

Healthcare organisation impacted by ransomware

A ransomware attack simultaneously affected **50 healthcare locations**, disrupting operations across multiple sites.

The organisation had maintained robust backups, allowing specialist recovery teams to restore systems without paying a ransom.

Operations were restored **within five days** and the total cost of recovery exceeded £323,000.

Total cost of the incident exceeded
£323,000

The incident highlights an important lesson: even well-prepared organisations can experience attacks, but preparation significantly improves outcomes.

Questions care providers frequently ask

hello@qcaregroup.co.uk | www.qcaregroup.co.uk

Q. *We are a small organisation. Why would criminals target us?*

Cyber criminals often target organisations based on vulnerability rather than size. Smaller organisations can be viewed as easier targets, while still holding valuable information.

Q. *We already have an IT provider. Isn't that enough?*

IT providers play a critical role in prevention and day-to-day management. However, major cyber incidents often require specialist forensic, legal, regulatory and communications support.

Q. *What is the biggest cyber risk facing care providers?*

There is no single answer. Most incidents involve a combination of technology, processes and human behaviour. Staff awareness remains one of the most effective forms of protection.

Q. *What should leaders focus on first?*

Start with the fundamentals: multi-factor authentication, staff training, tested backups and a clear incident response plan.

Leadership considerations for 2026

hello@qcaregroup.co.uk | www.qcaregroup.co.uk

The organisations best placed to manage cyber risk are those that treat it as a board-level issue rather than purely a technical challenge.

Leadership teams should regularly consider:

- ***What would happen if our systems were unavailable tomorrow?***
- ***How quickly could we continue delivering safe care?***
- ***How would we communicate with residents, families and regulators?***
- ***What support would we need during a major incident?***

The answers to these questions often reveal opportunities to strengthen resilience before an incident occurs.

Final thought...

Cyber risk is now part of the operating environment for every care provider.

While attacks cannot always be prevented, their impact can be significantly reduced through planning, awareness and preparation.

For organisations entrusted with the care of vulnerable people, cyber resilience is no longer optional. It is an essential part of delivering safe, sustainable and high-quality care.

THIS GUIDE WAS BOUGHT TO YOU BY

Quality Care Group

Specialists in care home insurance solutions since 2009.

332 Kingsway, Hove, East Sussex BN3 4QW | Tel: 01273 424 904

Registered in England & Wales. Registration No. 6874783