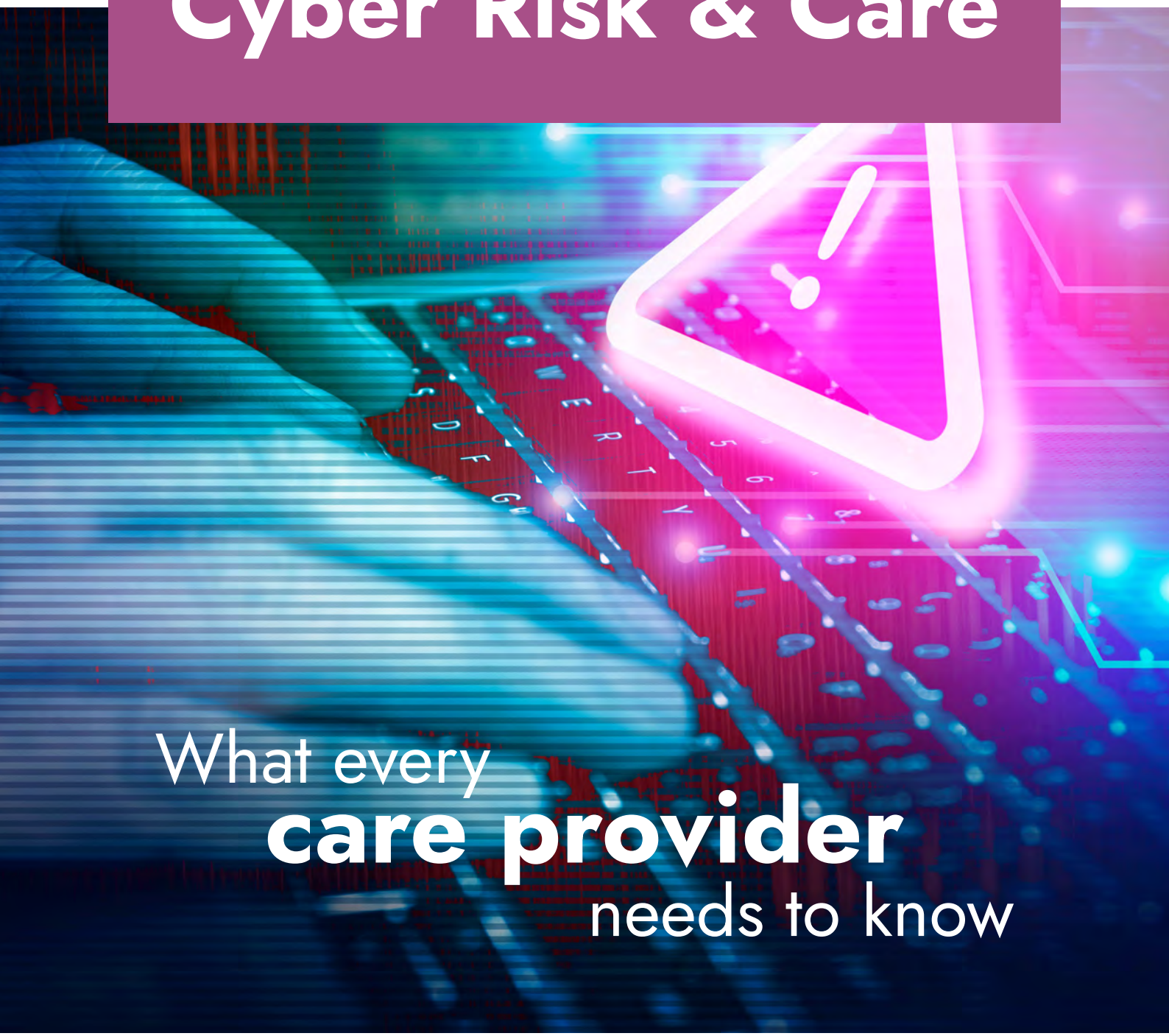
Quality Care Group

Cyber Risk & Care



What every **care provider** needs to know

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

A modern risk every care business faces

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

When care providers think about risk, they often picture fires, floods or accidents.

Yet today, the risk most likely to disrupt your organisation may be sitting behind a computer screen.

Cyber attacks are now one of the biggest operational threats facing UK care businesses. They can prevent staff accessing care records, disrupt medication management systems, expose sensitive resident data and create significant financial losses.

For organisations responsible for vulnerable people, the consequences can extend far beyond IT systems.

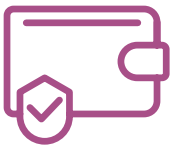
Why care businesses are being targeted

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

Cyber criminals are not only interested in large corporations.

They actively seek organisations that:

Hold sensitive personal information



Process regular financial transactions

Depend on systems that cannot afford downtime

May have limited in-house cyber security resources

Care providers often meet all four criteria.

Resident records, medication information, payroll data and financial details are valuable targets for criminals.

The reality of today's cyber threat

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

Many care operators still view cyber attacks as a technology issue.

In reality, they are a business continuity issue.

A successful attack can affect:

Resident Safety

If care records, medication systems or communication platforms become unavailable, staff may need to revert to manual processes with little warning.

Financial Stability

Ransom demands, system recovery costs and business interruption can quickly become significant.

Regulatory Compliance

Data breaches may trigger investigations by the Information Commissioner's Office, alongside wider scrutiny of governance and data protection arrangements.

Reputation

Families trust care providers with highly sensitive information. A public breach can damage confidence among residents, relatives, commissioners and staff.

Fire Risk vs Cyber Risk

FIRE RISK

Every care business understands the importance of fire protection.

Fire prevention measures are embedded throughout the sector and insurance protection is considered essential.

Yet cyber incidents are now statistically more likely to occur than a serious fire event, despite many providers having little or no dedicated protection in place.

This isn't about replacing traditional risk management.

It's about recognising that the threat landscape has changed.

CYBER RISK

The human factor

Technology is only part of the story.

Many cyber incidents begin with simple human interactions.

Examples include:

- **Clicking a malicious email link**
- **Opening an infected attachment**
- **Responding to fraudulent payment requests**
- **Using weak passwords**
- **Sharing information with someone posing as a trusted contact**

Staff awareness remains one of the strongest defences against cyber crime.

What good cyber resilience looks like

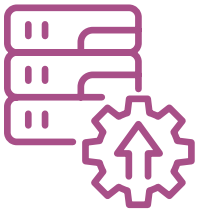
hello@qcaregroup.co.uk | www.qcaregroup.co.uk

There is no single solution that eliminates cyber risk.

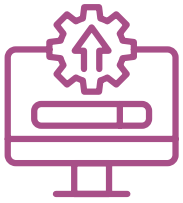
However, organisations can significantly reduce their exposure through practical steps:

Multi-factor authentication on key systems

Ongoing staff awareness training



Regular, tested backups



Prompt software updates

Strong password policies

Clear incident response procedures

The goal is not to become invulnerable.

The goal is to become harder to attack and quicker to recover.

When prevention isn't enough

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

Even organisations with strong controls can experience cyber incidents.

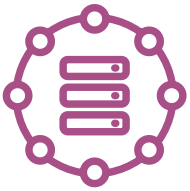
The difference often lies in how quickly they respond.

A major cyber event may require:

Specialist forensic investigators

Regulatory support

Legal advice



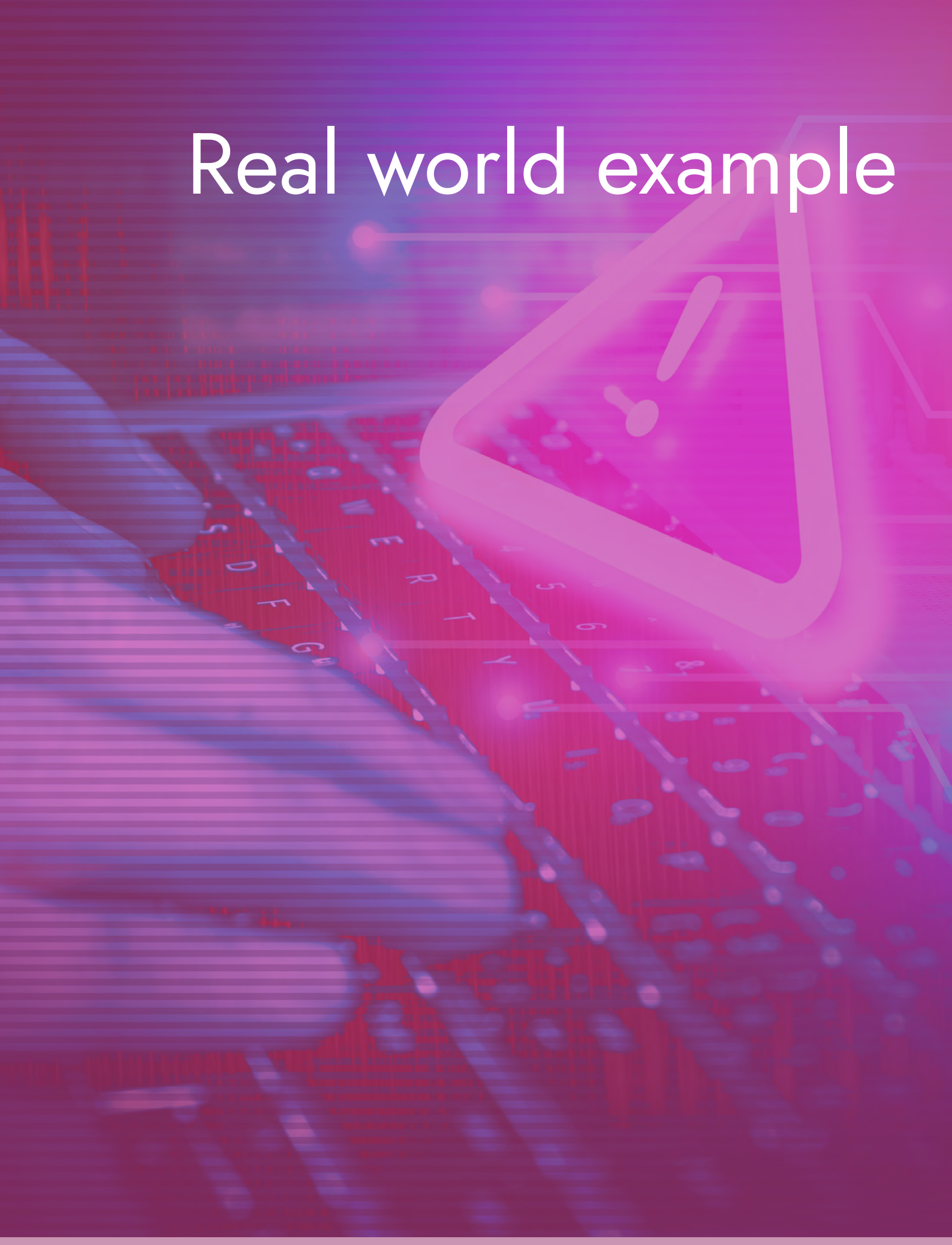
System restoration experts

Data breach management

Business continuity assistance

Having access to specialist support can dramatically reduce disruption and recovery time.

Real world example



Ransomware attack on a healthcare organisation

A ransomware attack simultaneously affected **50 healthcare locations**, locking critical systems and disrupting operations.

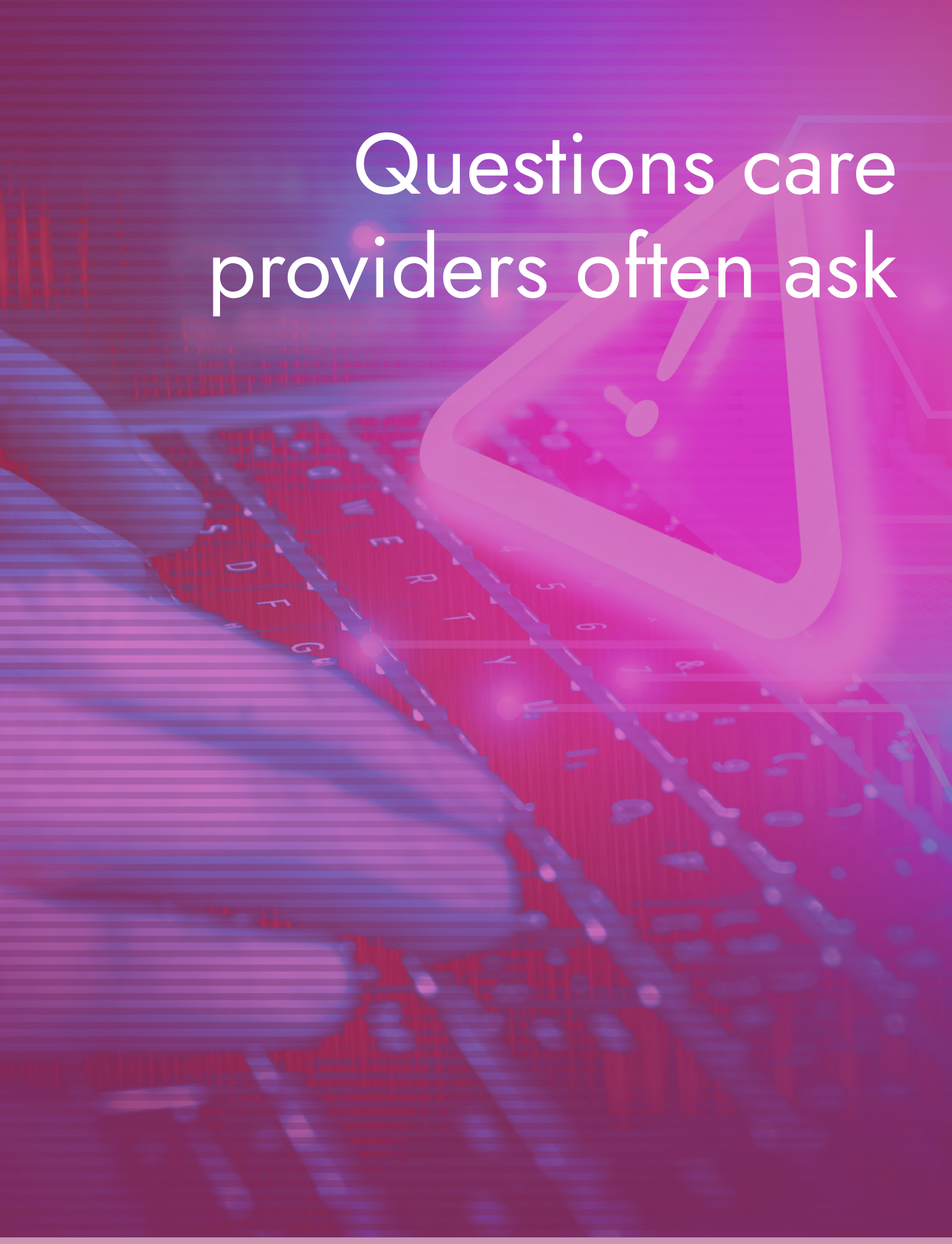
Because robust backups were in place, specialist response teams were able to **restore systems without paying a ransom**.

Business interruption costs and recovery expenses were covered, allowing normal operations to **resume within five days**.

Total cost of the incident exceeded £323,000

Without specialist support, recovery would likely have taken significantly longer.

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



Questions care providers often ask

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

We're a small organisation. Are we really a target?

Yes. Many cyber criminals actively target smaller organisations because they often have fewer resources dedicated to cyber security.

We have IT support. Isn't that enough?

IT support plays a vital role in prevention and day-to-day management. However, a major cyber incident often requires specialist forensic, legal and regulatory expertise beyond standard IT services.

How can we reduce our risk?

Focus on practical measures such as multi-factor authentication, regular backups, software updates and staff awareness training.

Does our existing insurance cover cyber attacks?

Many traditional insurance policies provide little or no protection for cyber incidents. Organisations should review their arrangements carefully to understand any gaps.

Final thought...

Cyber risk is no longer an IT issue.

It is a **leadership, governance** and **safeguarding issue.**

For care providers, preparation today can make the difference between a manageable incident and a major operational crisis tomorrow.

Understanding your exposure, strengthening your resilience and ensuring appropriate support is available before an incident occurs are all important parts of protecting your residents, your people and your organisation.

Don't leave your residents' data and your care home's future to chance.

Contact Quality Care Group today for a free, no-obligation consultation.

Call 01273 424 904 | **Click to request a quote**

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