Somerbys IT

Reducing Risk & Exposure

A Practical Guide for East Midlands Businesses

Why this guide exists

Cyber risk has changed.

For most businesses, it's no longer about a single "big hack" or a dramatic system failure. Risk tends to build quietly, often through everyday IT decisions, outdated systems, or processes that haven't been reviewed for years.

At Somerbys IT, we support businesses across Leicestershire, Nottinghamshire and Derbyshire, and one thing comes up time and time again:

Most cyber incidents we see could have been prevented with the right basics in place.

According to the UK Government's Cyber Security Breaches Survey 2024, 50% of UK businesses experienced a cyber security breach or attack in the last 12 months, with phishing being the most common entry point.

For businesses with 10–100 employees, the impact is often felt harder because downtime, data loss or disruption affects everyone.

This guide exists to help business owners:

- Understand where cyber risk actually comes from
- See how risk and exposure build over time
- Take realistic, achievable steps to reduce both

No scare tactics.
No technical waffle.
Just clear, practical advice you can act on.

"Most cyber incidents don't happen because businesses don't care. They happen because nobody has joined the dots."

Allan Page, MD Somerbys IT

What “risk & exposure” really mean in plain English

These two terms are often used together, but they mean different things.

Risk is the chance of something going wrong.
Exposure is how much damage it causes when it does.

A simple example:

- A phishing email landing in an inbox is a risk
- A staff member clicking it and losing access to systems for three days is exposure

You can never reduce risk to zero. But you can reduce exposure. And that’s what protects your business, your staff, and your customers.

Businesses that focus only on prevention often struggle to recover quickly. Businesses that understand exposure plan for when things go wrong, not if.

Why SMEs are being targeted more than ever

Cyber criminals don’t just go after large organisations. In fact, SMBs are often seen as easier targets.

Recent UK data shows:

- Over 40% of cyber attacks against UK businesses target small and medium-sized organisations (UK Government Cyber Security Breaches Survey 2024)
- The average cost of a cyber incident for a UK SME runs into thousands of pounds once downtime, recovery, and lost productivity are considered

Attackers know that many smaller businesses:

- Don’t have dedicated IT or security teams
- Rely on older systems that “still work”
- Assume they’re too small to be a target

Unfortunately, that assumption increases exposure.

Phishing remains the biggest entry point for attackers, with

84 %

of reported breaches starting this way.

Source: UK Government Cyber Security Breaches Survey 2024

The most common risk areas we see across East Midlands SMBs

While every business is different, the same patterns appear again and again.

1. Outdated or unsupported systems

Devices or software that no longer receive updates are one of the biggest contributors to cyber risk. Once support ends, security holes remain open permanently.

This includes:

- Older versions of Windows
- Unpatched servers or firewalls
- Legacy applications that haven't been reviewed

Attackers actively scan for these weaknesses because they're easy to exploit.

2. Weak access controls

Too many people having too much access is a major exposure risk.

We regularly see:

- Shared logins
- Former staff accounts still active
- Admin access given "just in case"

If one account is compromised, the damage spreads quickly.

3. Poor visibility of systems and data

Many businesses struggle to clearly answer:

- What systems do we rely on day to day?
- Where is our data stored?
- Who is responsible for maintaining each system?

Without visibility, risk is invisible too.

4. Backups that haven't been checked

Backups are essential, but only if they work when needed.

Common issues include:

- Backups running but not monitored
- No regular test restores
- Backups stored on the same system as live data

The **UK's National Cyber Security Centre** regularly highlights failed or incomplete backups as a key reason businesses struggle to recover after ransomware incidents.

Practical steps to reduce risk and exposure quickly

You don't need to fix everything at once. These steps deliver the biggest impact early on.

Start with the basics

- Ensure all devices and systems are fully supported and patched
- Remove or replace anything that's reached end-of-life

Lock down access

- Enable multi-factor authentication wherever possible
- Review who has access to what and remove anything unnecessary

Get confidence in your backups

- Confirm backups are running successfully
- Test restores regularly
- Ensure backups are protected from ransomware

Assign responsibility

- Make it clear who owns IT and cyber decisions internally
- Ensure risks are reviewed, not ignored

Even these steps alone can significantly reduce cyber risk exposure.

Turning cyber risk management into a habit

Reducing risk isn't a one-off IT project. The most resilient businesses treat it as an ongoing process.

This works best when:

- IT systems are reviewed regularly, not only when something breaks
- Staff understand their role in keeping the business secure
- Cyber risk is discussed at management level, not just left to IT

Proactive IT support helps spot problems early, before they become expensive or disruptive.

Next step: Get clarity on your real risk

If you want a clear, honest view of where your biggest risks sit and what to prioritise next, the best place to start is an independent review.

Book a Cyber Risk Assessment with Somerbys IT

We'll:

- Identify your key risk areas
- Explain them in plain English
- Provide practical recommendations tailored to your business

No pressure.
No jargon.
Just clarity, so you can make informed decisions with confidence.

0333 456 4431 | info@somerbysit.co.uk | www.somerbysit.co.uk

Dock 3, Space City
30 Exploration Drive
Leicester, LE4 5JU

Somerbys IT