Business Resilience
for SMEs

REAL RISK
SOLUTIONS

Risk and Resilience
Solutions

Grounded in Reality

Supplier Failure, Cyber Incidents and Practical Testing

Three questions every SME Leader should ask.

June 2026

Table of Contents

Supplier Failure, Cyber Incidents and Practical Testing

Many SME disruptions do not begin inside the business.

They arrive through a supplier, a technology provider, a cyber incident, a logistics failure, a key outsourced service or a dependency that has become so familiar it is barely noticed.

That is why practical business resilience needs to look beyond the four walls of the business.

For many SMEs, the most important question is not simply:

“What could go wrong here?”

It is:

“What do we depend on that could stop us delivering?”

That includes people, systems, suppliers, premises, data, outsourced services, specialist equipment, customer access, transport, finance, professional advisers and technology platforms.

Some of those dependencies are obvious.

Others only become obvious when something fails.

Supplier failure is often discovered too late

Supplier dependency is one of the most common areas of hidden exposure.

A business may know who its major suppliers are, but not always what would happen if one of them failed at short notice.

The practical questions are straightforward:

Which suppliers are essential to keeping the business operating?

Which products, materials, systems or services do they support?

How quickly would their failure affect customers?

Do we have a credible alternative?

Who would make the decision to switch supplier?

What contractual, quality, cost or lead-time issues would follow?

For many SMEs, supplier resilience is not about building a complex procurement risk framework.

It is about understanding where the business has concentrated dependency and where disruption would hurt first.

A single supplier may be acceptable.

A single supplier that nobody could replace quickly may be a serious exposure.

Cyber resilience is not just an IT issue

Cyber incidents are often discussed as technical events.

They are not.

A cyber incident can quickly become an operational, financial, customer, legal, insurance and reputational issue.

The IT response matters, of course.

But SME leaders also need to ask:

- Can we still contact customers?
- Can we access critical records?
- Can we continue taking orders?
- Can we pay staff and suppliers?
- Can we communicate internally?
- Who decides what we say externally?
- Who speaks to insurers, clients, regulators or advisers?
- What do we do if email or other comms channels are unavailable?
- What happens if systems are down for a day, three days or longer?

A cyber incident creates business decisions, not just technology decisions.

That is why cyber resilience needs to be discussed by the leadership team, not left entirely to the IT provider.

The question is not only, “Are we protected?”

It is also, “Could we operate, decide and communicate if protection fails?”

Testing reveals what documents often miss

Many SMEs have arrangements that look reasonable on paper but have never been walked through.

That is risky because disruption exposes gaps very quickly.

A short practical walkthrough can reveal:

- Unclear roles.
- Missing contact details.
- Over-reliance on one person.
- Assumptions about supplier availability.
- Unrealistic recovery times.
- Gaps in customer communication.
- Weaknesses in manual workarounds.
- Confusion about decision-making authority.
- Dependencies that were not previously visible.

Testing does not need to be elaborate.

Business Resilience for SMEs

For many SMEs, a simple 60-minute tabletop discussion is enough to generate valuable insight.

Take one realistic scenario and ask the leadership team:

- What has happened?
- What must keep working?
- Who is making decisions?
- Who needs to know?
- What do we do in the first hour?
- What do we do by the end of the day?
- What would stop us responding well?
- What needs to be improved?

This is not about catching people out.

It is about building confidence and finding practical gaps before a real disruption does.

Resilience should be proportionate

The best resilience work for SMEs is proportionate.

- It should not create unnecessary bureaucracy.
- It should not bury the business in documents.
- It should not use language that only risk specialists understand.
- It should help leaders see where the business is exposed and what to address first.

That usually means focusing on:

- Critical activities.
- Key dependencies.
- Realistic disruption scenarios.
- First-hour decisions.
- Customer and staff communication.
- Supplier alternatives.
- Cyber response beyond IT.
- Simple recovery actions.
- Clear ownership.
- A practical improvement plan.

The purpose is not to predict every event.

The purpose is to improve the business's ability to respond when something important is disrupted.

Business Resilience for SMEs

Three questions every SME should ask

A useful starting point is to ask three questions.

- First: **Which supplier failure would hurt us fastest**?
- Second: **Could we still operate and communicate during a cyber incident**?
- Third: **Have we actually tested what we would do**?

These questions are simple, but they often reveal the most important resilience priorities.

They help move the conversation away from generic planning and towards practical business solutions.

A practical next step

At Real Risk Solutions, we help SMEs identify where they are most exposed to disruption and what to address first, through a practical Rapid Resilience Diagnostic.

The diagnostic looks at the activities that matter most, the dependencies that could interrupt them, the scenarios that are most relevant and the first improvements that would make the biggest difference.

The output is not a large manual.

It is a clear view of priorities and a practical 90-day action plan.

Because resilience is not about having the perfect document.

It is about knowing what matters, what could fail and what to do first.

If you wish to discuss any of these matters and the implications for your business in more detail or require assistance in identifying what to do next, then contact Real Risk Solutions at resilience@realrisksolutions.