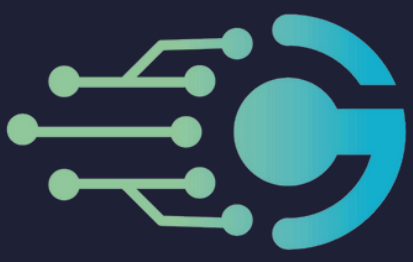
GUIDE

IT Exposure: The Hidden Risks Lurking in Everyday Business Systems



Chapman Technology Partners

Who this guide is for

This guide is aimed at business owners, managing partners, operations leaders, compliance managers and IT leads who deal with technology day to day and want to understand where risk quietly builds up.

Why this guide exists

Most IT exposure does not come from dramatic failures.
It builds slowly through:

- Everyday decisions
- Workarounds that become permanent
- Systems that no one quite owns anymore

By the time a problem is visible, the damage is often already done.
This guide helps you spot exposure before it turns into an incident.

Exposure is not the same as risk

Risk is the likelihood of something going wrong.
Exposure is the impact when it does.

For example:

- A phishing email is a risk
- A user with excessive access is exposure
- A system failure is a risk
- No tested backups is exposure

Many firms focus on preventing threats but overlook how vulnerable they would be if those threats succeed.

Common places exposure creeps in

1. Access that has never been reviewed

Staff often accumulate access over time.
Roles change. People move teams. Permissions stay.

This leads to:

- Excessive access
- Weak segregation of duties
- Higher impact if an account is compromised

Access control is one of the most overlooked exposure points we see.

2. Systems that are “too awkward to change”

Legacy platforms are rarely reviewed because:

- They still work
- They support critical processes
- No one wants the disruption

But these systems often:

- Lack modern security controls
- Depend on outdated infrastructure
- Sit outside normal monitoring

They quietly increase exposure every year they remain untouched.

3. Shadow IT and workarounds

When systems don't quite fit the business, staff find alternatives.

This can include:

- Personal file sharing tools
- Unapproved apps
- Local data storage
- Informal processes

Each workaround feels harmless. Collectively, they create blind spots.

4. Backups that exist but haven't been tested

Many firms believe they are protected because backups are "in place".

The real questions are:

- Are they monitored?
- Are they tested?
- Can they actually restore what matters?

Untested backups are one of the biggest exposure risks in a real incident.

5. No clear ownership of IT decisions

Exposure increases when:

- IT decisions are fragmented
- Responsibility is unclear
- Changes happen without oversight

When no one owns the whole picture, risk hides in the gaps.

Why “nothing has happened yet” is not reassurance

The most exposed firms we work with often say the same thing:
“We’ve never had a serious issue.”

That usually means:

- Weaknesses have not been tested
- Luck has played a part
- Warning signs have been missed

Exposure is highest **just before** an incident, not after.

Reducing exposure does not mean replacing everything

This is important.

Reducing exposure is about:

- Understanding what you already have
- Fixing the weak points
- Removing unnecessary risk
- Making informed decisions

Most improvements are practical, not dramatic.

Turning exposure into clarity

A structured review of systems, access and controls helps to:

- Identify where exposure actually sits
- Prioritise what matters most
- Reduce risk without disruption
- Support regulatory expectations

It replaces assumptions with facts.

If you want to understand where exposure is quietly building across your IT systems, an independent review will give you the clarity you need to act with confidence.

Get in touch with the experts at Chapman Technology Partners.

Chapman Technology Partners

Strategic IT, Cyber Security & AI Solutions for Regulated Firms

Strawberry Fields Digital Hub,
Chorley, PR7 1PS

enquiries@ctpartners.co.uk
01257 542388

www.chapmantechnologypartners.co.uk

CYBER ESSENTIALS CERTIFIED