Chapter 10: Five simple ways clients can reduce cyber risk

Cyber resilience isn't about eliminating every risk

It's about making life harder for cybercriminals and making recovery easier if something goes wrong.

74% of SMEs plan to take some form of cyber action in the next year.

1. Turn on multi-factor authentication (MFA)

Think of MFA as an extra lock on the front door.

Even if a criminal steals a password, MFA can make it much harder for them to gain access.

Many cyber incidents begin with compromised credentials, making MFA one of the simplest and most effective controls available.

Broker conversation starter

"Where is MFA currently switched on within your business and crucially, where isn't it?"

60 Second Claim Example

An employee clicked a phishing link and entered their credentials, including their multi-factor authentication code. This resulted in a compromised account and follow-on phishing activity.

While the incident was contained quickly, the organisation still needed specialist support and investigation.

Broker takeaway: Security controls significantly reduce risk, but they do not eliminate it. Preparation and response remain important.

Typical Cover Sections

- ✓ Incident Response Services
- ✓ Privacy & Security Liability involving regulatory investigations if the impact extends beyond the initial compromise.

---

2. Back up critical data

If a business loses access to systems, backups can make the difference between inconvenience and catastrophe.

But here's the important bit: Backups need to be tested.

There's little comfort in having a backup strategy if nobody knows whether it works.

Broker conversation starter

"When was the last time you tested the restoration of your backups?"

---

3. Train people, not just systems

Most attacks still involve human interaction:

- A clicked link
- A trusted email
- A fraudulent payment request

People are often the first and last line of defence and one of the most important.

Cyber awareness doesn't need to be complicated. It needs to be regular.

Employee error ranks among SMEs' top three cyber risks, yet a third provide no cyber-security training.

Broker conversation starter

"How confident are staff in identifying a suspicious email?"

60 Second Claim Example

A finance employee received what appeared to be a legitimate security request and entered their credentials. The account was compromised and used to send convincing messages to customers and other contacts.

The incident required investigation, customer communications and a review of what information may have been accessed.

Broker takeaway: Good businesses with security controls and experienced staff can still be caught out by sophisticated phishing attacks.

Typical Cover Sections

- ✓ Incident Response Services
- ✓ Notification Services
- ✓ Privacy & Security Liability
- ✓ Regulatory Investigations & Fines

---

4. Know your critical suppliers

Think about:

- Cloud providers
- Software vendors
- Payroll systems
- Managed service providers
- Accounting platforms
- Payment providers

If one of those suppliers experiences a cyber incident, the impact can quickly spread.

Understanding these dependencies is an important part of cyber resilience.

Broker conversation starter

> **"How would you continue operating if a key supplier became unavailable tomorrow?"**

---

5. Have an incident response plan

The best plans aren't necessarily complicated.

They're clear.

- Who makes decisions?
- Who gets called?
- Who communicates with customers?
- Who manages recovery?

Answering those questions before an incident can significantly improve the response.

Many cyber policies provide access to pre-breach support such as virtual CISO services, awareness training, exposure assessments and incident response planning tools. These services help businesses understand their cyber risk and build a practical response plan before they are under pressure.

Why cyber insurers ask about security

The goal is not perfection. It's understanding risk.

For example:

- Evidence of reasonable cyber hygiene
- Controls that match the size of the organisation
- Controls that match the exposure
- Willingness to improve
- Awareness of critical risks

Client says / Reality says

Client says:
"We're not technical enough to improve our cyber security."

Reality says:
You don't need an enterprise-sized IT budget to improve cyber security. Many businesses already have access to core security features through platforms such as Microsoft 365 and Google Workspace. Combined with good processes, planning and staff awareness, these can provide a strong foundation for reducing cyber risk. Small improvements can make a significant difference.

Key takeaway

Cyber resilience doesn't start with buying technology.

It starts with asking better questions about:

- Strong passwords
- MFA
- Backups
- Awareness
- Planning

Together they can make a business significantly harder to attack and much easier to recover.

Want to explore this further?

Visit the Cyber Knowledge Hub:

Why Do Cyber Insurers Insist on IT Security?
A practical explanation of why insurers ask about controls such as MFA, backups and access management.

Why Multi-Factor Authentication (MFA) Matters
One of the simplest and most effective cyber protections available.

How Cybercriminals Exploit MFA Reset Prompts
Demonstrates how criminals often target processes around security controls rather than the controls themselves.

How Cybercriminals Exploit MFA Reset Prompts
Learn why good controls still need good processes.

Why Do People Fall for Phishes?
A useful resource for understanding the human side of cyber risk.

Privileged Access Management Is a Critical Element of Internal Cyber Security
An introduction to managing access to critical systems and information.