Chapter 1: Why cyber is no longer optional

Let's start with one client

Think about one of your clients.

Not the largest.

Not the most sophisticated.

Just a typical client.

Now imagine they walk into work tomorrow and discover they can't:

- Access email
- Log into their systems
- Process payments
- Raise invoices
- Access customer records
- Contact suppliers

How long could they continue operating normally? An hour? A day? A week?

For many businesses, the honest answer is: **Not very long.**

And that's why cyber insurance matters.

A third of SME decision-makers fear their business might not survive a cyberattack.

Nearly 2 in 5 SMEs say their cyber security is unprepared to keep pace with growth.

The cyber conversation most brokers have heard

"We're too small."

"Our IT company looks after that."

"We don't have anything worth stealing."

"We're not a target."

These common objections are some of the biggest cyber myths.

Modern cybercriminals aren't always looking for the biggest business.

They're looking for the easiest opportunity. Increasingly this involves a smaller business directly, or via a supply chain.

Client says / Reality says

Client says:
"We're too small to be targeted."

Reality says:
Cybercriminals don't need to choose victims one by one anymore. AI has accelerated automated phishing campaigns, credential theft and supply chain attacks allowing them to target thousands of organisations at once.

Here's the uncomfortable truth

Every business is now a technology business.

The retailer, the manufacturer, the accountant.

Different industries. Same dependency

If technology stops, the business feels it.

And that's why cyber risk is no longer an IT issue.

It's a business resilience issue.

55% of SMEs say larger clients now expect them to meet their cyber security standards.

Broker conversation starter

The next time you're talking to a client, don't start with: "Do you buy cyber insurance?"

Start with:

"What happens to your business if your technology stops working tomorrow?"

The answer will usually tell you everything you need to know.

Key takeaway



Cyber risk follows dependency.

If a client relies on technology to communicate, trade, get paid or serve customers, they already have a cyber exposure.

That's why every broker should be having the conversation.

Want to explore this further?

Visit the Cyber Knowledge Hub:

Addressing the Cyber Gap with SMEs
Why many businesses still underestimate their exposure.

Overcoming Barriers to Buying Cyber Insurance for SMEs
Common client objections and how to challenge them.

From Corner Shops to Corporates: Why Every Business Is Now a Tech Company
A deeper look at why cyber risk follows business dependency.