# Chapter 9: Turning client objections into better cyber conversations

### Let's be honest

Cyber Insurance can feel complicated, technical and expensive.

But most objections are not final decisions. They are signs that the client has not yet connected cyber risk to their own business.

A good objection response does three things:

- ✓ It listens to the concern
- ✓ It reframes the issue in business terms
- ✓ It opens the next conversation

The best cyber conversations start with a better question.

---

## "We're too small."

### What they are really saying

"I do not think this applies to us."

This is probably the most common objection. It is also one of the most important to challenge carefully.

Many smaller businesses do not see themselves as attractive targets. They may assume cybercriminals are only interested in large companies, household names or businesses holding huge volumes of sensitive data.

But cybercriminals do not always look for the biggest business. Often, they look for the easiest opportunity.

A small business may still rely on email, online banking, cloud software, payment systems, supplier relationships and customer information. If any of those stop working, the business can feel the impact quickly.

### Broker conversation starter

Do not start by debating whether the client is a target. Start with dependency. Ask:

**"If your systems stopped working tomorrow, what would be affected first?"**

This moves the conversation away from company size and towards business impact.

The client may talk about:

- Not being able to invoice
- Not being able to take payments
- Staff being unable to work
- Customers not being served
- Delays to orders or projects
- Lost income

Once the client can see the dependency, cyber risk becomes much more relevant.

**"The size of the business is not the only issue. The better question is how much disruption a cyber incident could cause."**

---

## "Our IT company handles that."

### What they are really saying

"I think cyber risk is a technology problem for our IT provider to solve"

IT providers are an important part of cyber resilience. But a serious cyber incident can quickly become more than a technology problem.

A business may need to think about:

- Legal obligations
- Preserving evidence
- Regulatory reporting
- Customer communications
- Lost income
- Recovery costs
- Supplier disruption
- Claims support

**26% of businesses believe cyber may already be covered elsewhere or that their IT provider protects them.**

An IT provider may not be responsible for legal advice, regulatory notifications, customer communications, cybercrime losses or business interruption.

### Broker conversation starter

Do not dismiss the IT provider. Ask:

**"Who helps if the incident becomes more than a technology problem?"**

This helps the client understand that cyber insurance is not trying to replace IT support. It is designed to sit alongside it.

**"A good IT provider is important, but cyber incidents often create legal, financial, regulatory and communications challenges too. Cyber insurance helps bring the wider support together."**

Do not make this an IT versus insurance conversation. Make it about the wider response the business may need.

---

"We don't have anything worth stealing."

## What they are really saying

"I think cyber risk is only about data."

Many clients hear "cyber" and immediately think about stolen customer data. But cyber risk is broader than data theft.

**26% of SMEs say holding little sensitive is a main reason not to buy cyber insurance.**

Cybercriminals may target:

- Payment processes
- Email accounts
- Login details
- Supplier relationships
- Business operations
- Employee information
- Client communications

And sometimes attackers do not need to steal anything to cause serious disruption. If a business cannot access systems, communicate with customers or continue trading, the impact can be immediate.

## Broker conversation starter

Move the discussion from data to disruption. Ask:

**"What would be more painful: losing your data or losing access to your business for a week?"**

This helps the client think about cyber as an operational risk, not just an information risk.

**"Cyber risk is not only about what criminals might steal. It is also about what the business could lose access to."**

If the client says they do not hold valuable data, talk about access, operations and income.

---

## "We've never had a cyber incident."

### What they are really saying

“I do not see this as likely enough to worry about.”

Many businesses have never had a major cyber incident. But that does not mean the exposure is not there.

Many businesses have also never had a serious fire, flood or liability claim. They still insure against those risks because the impact could be significant if they happened.

Cyber insurance works in the same way. The question is not whether something has happened before.

The question is whether the business could respond and recover if something happened tomorrow.

### Broker conversation starter

Do not focus on fear. Focus on preparedness. Ask:

**”If something happened tomorrow, how quickly could the business recover?”**

This moves the conversation away from probability and towards resilience.

The client may start thinking about:

- Who would make decisions ?
- Who would contact customers ?
- Whether backups work
- Whether suppliers could help
- How long the business could trade without systems
- What cashflow impact downtime could create

**”Past experience does not remove future risk. The real question is whether the business could recover if something happened tomorrow.”**

Do not argue about whether the client will suffer an incident. Help them think through what recovery would look like.

---

## "Cyber insurance is too expensive."

### What they are really saying

"I don't see the value."

Cost always matters. But if the conversation starts and ends with premium, the client may never understand what they are actually buying.

Cyber insurance is not just a payment after a loss. It can provide access to expertise, support and a plan when a business is under pressure.

A cyber incident can create costs linked to:

- Business interruption
- System recovery
- Forensic investigation
- Legal advice
- Customer notification
- Regulatory response
- Specialist support
- Fraud recovery
- Reputation management

**Price is the single most influential provider-selection factor for 55% of SMEs.**

The value of cyber insurance is often easier to explain when the client understands what help they would need.

### Broker conversation starter

Do not simply compare premium to a worst-case loss. Ask what the client would be most worried about.

**"What would concern you most after a cyber incident?"**

The answer helps tailor the conversation.

- If they say lost income, talk about business interruption
- If they say customers, talk about communications and response support
- If they say regulators, talk about legal and regulatory support
- If they say systems, talk about recovery and restoration

**"It is worth thinking about cyber insurance not only as a cost, but as access to specialist help including legal, digital, ransom negotiation and communications services when the business needs it most. Policies also include tailored pre-breach advice and training to best mitigate the risk of an incident."**

Do not sell the cheapest answer. Help the client understand what problem they are trying to solve.

---

## "Cyber insurance requirements are too complicated."

### What they are really saying

"I am worried we will not qualify, or that this will be too difficult."

Some clients assume cyber insurance comes with unrealistic security expectations.

They may worry they need a large IT team, expensive tools or perfect cyber security before they can even have a conversation.

The goal is not perfection. The goal is understanding risk.

Insurers generally want to see reasonable cyber hygiene that matches the size, complexity and exposure of the business.

### Broker conversation starter

Reassure the client that improvement can be gradual. Ask:

**"Which cyber controls do you already have in place?"**

Then explore the basics:

- Multi-factor authentication
- Backups
- Staff awareness
- Supplier dependency
- Incident response planning

Many clients may already have more in place than they realise.

**"Cyber insurance does not require every business to look the same. The aim is to understand the risk and identify sensible, proportionate controls."**

Do not let the client assume cyber security has to be perfect. Help them see what they already have and what they could improve.

---

## "Just send me some information."

### What they are really saying

"I am not convinced enough to have the conversation yet."

This is one of the most typical ways  for a cyber conversation to stall.

The client may genuinely want more information. But sometimes this is a polite way of ending the discussion.

If you send a generic policy summary, the client may not read it or may not see why it applies to them.

A better approach is to send something specific to the concern they have raised.

### Broker response

Before sending anything, ask one more question.

**"Of course. What would be most useful: something on claims examples, common cyber incidents, or what cyber insurance actually helps with?"**

You could follow up with:

- A short claims example
- A sector-specific risk example
- A simple explanation of what happens during an incident
- A myth-busting piece on one of their objections
- A link to a relevant Cyber Knowledge Hub article

**"I'll send something practical rather than a long policy summary. It may help to look at how this type of incident affects businesses like yours, then we can pick the conversation back up."**

Do not let "send me some information" become the end of the discussion. Use it as a bridge to a better follow-up.

---

## A simple objection-handling framework

### 1. Acknowledge

Show that you have heard the concern.

"That is a fair point."

"A lot of businesses say the same thing."

### 2. Reframe

Move the conversation from cyber jargon to business impact.

"The question is not just whether you are a target. It is what would happen if your business was disrupted."

"This is not only an IT issue. It can become a legal, financial and operational issue too."

"The value is not just in the policy. It is in the support available when something goes wrong."

### 3. Ask the next question

Use a question that helps the client apply the risk to their own business.

"What would stop first if your systems went down?"

"Who would coordinate the response?"

"What would concern you most after an incident?"

The aim is to help the client see the relevance.

### Key takeaway



**Most objections are not really objections. They are signals.**

They show where the client needs more clarity, more context or a more relevant example.

The best cyber conversations are not about having the perfect rebuttal. They are about asking the next useful question.

### Want to explore this further?

Visit the Cyber Knowledge Hub:

**Overcoming Barriers to Buying Cyber Insurance for SMEs**
A detailed look at the misconceptions that commonly prevent businesses from buying cyber insurance.

**Addressing the Cyber Gap with SMEs**
Why so many businesses remain exposed despite increasing reliance on technology.

**From Corner Shops to Corporates: Why Every Business Is Now a Tech Company**
Practical examples of why cyber risk affects organisations regardless of size or sector.

**Why Do Cyber Insurers Insist on IT Security?**
A practical explanation of why insurers ask about reasonable cyber controls.