Chapter 11: Five cyber questions every broker should ask

You don't need to be a cyber expert to ask these questions.

And you definitely don't need to become your client's IT consultant

You do need to:

- ✓ **Help clients understand risk**
- ✓ **Help them understand impact**
- ✓ **Help them make informed decisions**

Often that starts by asking better questions.

Question 1

"What happens if your systems stop working tomorrow?"

This is usually the best place to start.

It moves the conversation away from technology and towards business impact.

Clients rarely know what ransomware is.

They absolutely know what happens when they can't trade.

Question 2

"Which technology could your business least afford to lose?"

- Email?
- Payments?
- Customer records?
- Production systems?
- Cloud software?

Every answer reveals something about cyber exposure.

And every answer creates a useful conversation.

Question 3

"Who would you call first after a cyber incident?"

Many businesses assume the answer is IT. But serious cyber incidents often involve:

- Legal advice
- Forensic investigations
- Customer communications
- Regulatory issues
- Business interruption

The answer can tell you a lot about how prepared a client really is.

Question 4

"Which supplier would cause your business the biggest disruption if they couldn't operate?"

Cyber risk isn't limited to the business itself.

Many organisations depend heavily on technology providers, cloud platforms and third-party suppliers.

Sometimes the biggest cyber risk sits outside the organisation entirely.

Question 5

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

Some clients worry about:

- Lost income
- Lost customers
- Regulatory issues
- Damaged reputation
- Operational disruption

Understanding what matters most to the client often makes the cyber conversation more productive.

Client says / Reality says



Client says:
"I don't really understand cyber risk"

Reality says:
They don't need to. Most cyber risk conversations are really business conversations about dependency, disruption and resilience.

Key takeaway



Brokers do not need to be cyber experts to start a valuable cyber conversation.

Five simple questions can help identify the client's reliance on technology, the systems and suppliers it cannot operate without, its preparedness for an incident and the consequences it is most concerned about.

The broker's role is to help the client connect cyber risk to business impact and make an informed decision. When the conversation becomes more technical, Brit's cyber team can provide the specialist support needed to take it further.

Want to explore this further?

Visit the Cyber Knowledge Hub:

📖 **Addressing the Cyber Gap with SMEs**
Practical insights into why brokers play such an important role in cyber education.

📖 **Overcoming Barriers to Buying Cyber Insurance for SMEs**
Useful guidance for handling common client objections.

📖 **From Corner Shops to Corporates: Why Every Business Is Now a Tech Company**
A useful resource for helping clients understand why cyber risk exists regardless of size.