# Chapter 3: Cyber risk looks different for different businesses

### Think about your last three client meetings

Perhaps a solicitor, an accountant and a manufacturer.

At first glance, they may not have much in common.

But ask one question and the connection becomes clearer:

What happens if their technology stops working?

Different businesses. Different impacts. Same underlying dependency.

Organisations now rely on technology to communicate, trade, get paid, serve customers and work with suppliers. Cloud software, online banking, digital suppliers and AI-powered applications may look different from sector to sector, but they create a shared exposure.

That is why cyber risk follows dependency, not sector. Every business may have cyber risk. The difference is how that risk shows up.

---

### 1. The legal firm

- A solicitor's business runs on trust
- Client confidentiality
- Sensitive information
- Fund transfers
- Regulatory obligations

A cyber incident can quickly become more than an IT problem. It can disrupt client relationships, affect operations and create significant reputational challenges.

Law firms are increasingly attractive targets because of the sensitivity of the information they hold. Where client data has been accessed or stolen, the threat of publication can create intense pressure to resolve the incident quickly, particularly when confidentiality and client relationships may be affected.

### Broker conversation starter

> **"What information would cause the biggest issue if it became public?"**

---

### 2. The accountancy firm

- Accountants sit at the centre of some of the most sensitive financial information a business owns
- Payroll
- Tax records
- Financial statements
- Banking information

Cybercriminals know this. That's why accountancy firms are often attractive targets for phishing, credential theft and payment fraud.

#### Broker conversation starter

> **"How would your clients be affected if you couldn't access their records for several days? How would this affect key deadlines such as tax or regulatory filings?"**

---

### 3. The manufacturer

- Manufacturers often think cyber is a data problem
- In reality, it can be an operational problem
- If systems are unavailable, production lines can stop
- Orders may be delayed
- Customers may be impacted

For many manufacturers, the cost of downtime can quickly outweigh the cost of the original attack.

#### Broker conversation starter

> **"Could you cope with losing data or losing production for a week?"**

---

### 4. The retailer

- Retailers depend on transactions
- Payment systems
- Inventory platforms
- E-commerce websites
- Customer data
- When those systems fail, revenue can stop almost immediately

Cyber incidents don't need to involve a major data breach to create a major business problem.

Sometimes the disruption alone is enough.

#### Broker conversation starter

> **"How long could you trade if your payment systems went offline?"**

## Client says / Reality says



**Client says:**
*"Cyber isn't really a concern for our industry."*

**Reality says:**
Cyber incidents don't target industries. They target opportunities. The impact might look different in a law firm than it does in a factory, but almost every business now relies on technology to operate.

## Key takeaway



**Different businesses experience cyber risk differently.**

- A solicitor worries about confidentiality.
- A manufacturer worries about production.
- An accountant worries about financial information.
- A retailer worries about transactions.

But they all rely on technology.

Every business is now a technology business.

And that's why cyber risk and insurance is a business resilience conversation for almost everyone.

### Want to explore this further?

**Visit the Cyber Knowledge Hub:**

📖 **Cyber Risk in Legal Firms: Talking Points for Brokers and Businesses**
Practical guidance on the cyber risks facing legal practices.

📖 **Why Cyber Risk Matters for Accountancy Firms**
Explores the unique cyber exposures within accountancy practices.

📖 **Cyber Risk Presents Material Risk for Manufacturing**
A closer look at operational disruption and manufacturing cyber exposures.

📖 **From Corner Shops to Corporates: Why Every Business Is Now a Tech Company**
Why cyber risk is increasingly driven by technology dependency rather than company size or sector.