Chapter 2: The incidents your clients are most likely to face

Most cyber incidents start with something simple:

- An email
- A text message
- A phone call
- A payment request
- A trusted supplier

Cybercriminals don't always break in.

Quite often, they're let in.

44% of SMEs fear a cyberattack on a supplier could stop them trading.

The four incidents every broker should understand

1. Payment fraud

- → A member of the finance team receives a request to make an urgent payment
- → Everything looks genuine
- → The email signature is right
- → The timing feels right
- → The payment is made
- → The money is gone

These attacks often rely on impersonation and trust rather than technical hacking.

Broker conversation starter

> **"What controls are in place if somebody asks to transfer £5,000 today?"**

60 Second Claim Example

A professional services firm discovered they had transferred funds to a fraudulent bank account after receiving altered payment instructions from a threat actor. The payment appeared genuine and followed an existing transaction.

The result was a significant financial loss, an urgent investigation and the involvement of legal and cyber specialists to establish what had happened and whether any funds could be recovered.

Broker takeaway: Businesses do not need to suffer a system breach to experience a cyber loss. A convincing email can be enough.

Typical Cover Sections

- ✓ Cybercrime & Funds Transfer Fraud
- ✓ Incident Response Services
- ✓ Potentially Privacy Liability and Regulatory Defence Costs if third-party claims or regulatory investigations emerge.

This demonstrates that cyber policies often respond through several sections at the same time, rather than a single insuring clause.

---

2. Ransomware

- A link is clicked
- A password is compromised
- An attacker gains access
- Systems are encrypted
- Operations grind to a halt
- Headlines focus on the ransom demand

Businesses usually feel the pain from lost trading, downtime and recovery costs.

Ransomware can also create privacy and regulatory exposure where data has been accessed or stolen and the threat actor threatens to publish it. If sensitive information is released, the impact can extend to reputational harm, regulatory scrutiny and potential privacy claims. Cyber insurance can help with the legal costs of defending the insured, as well as settlements arising from privacy actions or class actions.

Broker conversation starter



"How long could your business operate if staff couldn't access systems for a week?"

60 Second Claim Example



A law firm suffered a ransomware attack which left it unable to access most of its data and systems. The attackers claimed to have stolen information and threatened further action.

Recovery required specialist forensic investigation, legal support and system restoration. The cost of the response quickly exceeded the cost of the technology affected.

Broker takeaway: The biggest cost of ransomware is often the disruption to the business, not the ransom itself. Although breach response costs are typically incurred within the first 24-48 hours, business interruption costs and class actions claims take longer to develop. and are often the most expensive cost of a ransomware claim.

Typical Cover Sections

- ✓ Incident Response Services
- ✓ Data Restoration
- ✓ Cyber Extortion
- ✓ Privacy & Liability Covers
- ✓ Business Interruption

---

3. Data breaches

- Not every attacker wants money immediately
- Sometimes they want information
- Customer data
- Employee records
- Commercial information
- Intellectual property

The costs often extend far beyond the breach; including investigations, notifications and reputational damage.

Broker conversation starter



"What information would cause the most damage if it became public tomorrow?"

---

4. Supplier incidents

- This is the one many businesses forget
- Your client may do everything right
- But what happens if a software provider, cloud platform or outsourced service provider suffers a cyber incident?

Broker conversation starter



"Which supplier would cause the biggest disruption if they went offline for a week?"

60 Second Claim Example



A business was unable to access critical data after a third-party software provider suffered a cyberattack. The organisation's own systems had not been compromised.

Despite this, operations were disrupted while the supplier investigated and restored services.

Broker takeaway: Cyber risk does not stop at the edge of a company's network. Suppliers can become a single point of failure. Breaches increasingly stem from vendors or suppliers and not insureds themselves.

Typical Cover Sections

- ✓ Incident Response Services
- ✓ Business Interruption

Client says / Reality says

Client says:
"We've never had a cyber incident."

Reality says:
Most businesses haven't experienced every major risk they insure against. The important question isn't what happened yesterday. It's whether the business could cope tomorrow.

52% of SMEs recognise that attackers could target them to reach a larger client.

Key takeaway

Most cyber incidents start with ordinary business activities:

- Opening emails
- Making payments
- Trusting suppliers
- Responding to requests

A single incident can lead to operational disruption, financial loss, privacy issues and the need for several areas of cyber cover.

For brokers, the important question is not simply how an incident might happen, but how it could affect the client's ability to operate and recover

Want to explore this further?

Visit the Cyber Knowledge Hub:

Common cyberattacks and threat actors
A practical overview of phishing, ransomware, social engineering and common attack techniques.

Why do people fall for phishes?
Explains why phishing works and why intelligent people still get caught out.

The Rise and Rise of Social Engineering
How cybercriminals exploit trust, urgency and human behaviour.

The MOVEit Transfer Event and the Corresponding Impact
A useful example of how supplier and third-party risk can affect organisations of every size.

Dissecting Ransomware
A deeper look at why ransomware is much more than a ransom demand.