Chapter 7: What happens when a client calls for help?

The call nobody wants to make

- It's 8:17am on a Tuesday
- A client phones
- Staff can't access systems
- Emails have stopped working
- A ransom demand has appeared on screen
- Nobody knows what to do next

Who takes control?

For most businesses, this is the moment panic starts to set in. But for a well-managed cyber response, it's the moment specialists step in.

The first few hours matter most

One of the biggest misconceptions about cyber incidents is that they're purely technology problems.

They're not.

Within hours of an incident, a business may need to make decisions about:

- Containing the attack
- Preserving evidence
- Legal obligations
- Customer communications
- Regulatory reporting
- Business continuity

The insured should contact the 24-Hour Breach Response Hotline as soon as possible and refer to their policy for how to notify insurers - this is usually by email to a specific address. Early engagement helps bring in the right specialists, preserve evidence and avoid decisions in the first few hours that could increase downtime or complicate the forensic investigation. Claims can become harder to manage where businesses try to fix matters internally before insurers are involved.

What happens next?

While every incident is different, a typical response often looks something like this:

Step 1: Assess the situation

The immediate priority is understanding what has happened and what might still be happening.

Questions include:

- How did the incident occur?
- What systems are affected?
- Is the threat still active?
- Is sensitive information involved?

Step 2: Contain the problem

The next goal is limiting further damage.

That might involve:

- Isolating systems
- Restricting access
- Investigating compromised accounts
- Stopping the incident from spreading

Step 3: Coordinate the response

Once the immediate threat is understood and contained, the focus turns to managing the wider incident.

This may involve:

- Legal and regulatory advice
- Understanding notification obligations
- Coordinating forensic investigations
- Managing communications with customers and stakeholders
- Supporting decision-making during the incident

Step 4: Recover and restore

The focus shifts from managing the incident to getting the business back up and running.

Support may include restoring systems, managing disruption and coordinating ongoing recovery.

The question changes from: "What happened?" to: "How do we get back to business?"

Client says / Reality says

Client says:
"Our IT provider would sort that out."

Reality says:
A cyber incident can quickly become a technical, legal, regulatory, financial and reputational issue. Businesses often need several specialists working together simultaneously.

You won't be dealing with just one expert

Think of a cyber incident like a major emergency.

You wouldn't expect one person to do everything.

Depending on the incident, support may include:

- **Breach counsel**
- **Digital forensics experts**
- **Negotiation specialists**
- **Communications specialists**
- **Claims professionals**

We'll look at these specialists in more detail in the next chapter.

Broker conversation starter

Ask your client:

"If your business suffered a serious cyberattack tomorrow, who would coordinate the response?"

Many organisations have never considered the answer.

Key takeaway

The first few hours of a cyber incident can shape the cost, disruption and outcome.

Early notification allows the response services to assess what has happened, contain the threat, preserve evidence and coordinate the technical, legal, regulatory and communications response. Once the immediate threat is controlled, attention turns to restoring systems and getting the business operating again.

Cyber insurance helps clients answer three urgent questions:

- How do we stop this getting worse?
- How do we get back up and running?
- How do we manage the wider financial, legal and operational impact?

Want to explore this further?

Visit the Cyber Knowledge Hub:

📖 **Breach Response: Leave It to the Experts**
Explains the critical role of breach counsel during an incident.

📖 **Digital Forensics: Managing an Online Crime Scene**
Shows how investigators uncover what happened and help contain incidents.

📖 **Ransomware Negotiation: Don't Try This at Home**
Demonstrates why specialist expertise matters when dealing with threat actors.