Chapter 6: What cyber insurance actually does

Let's clear something up

Ask 10 people what cyber insurance does and you'll probably get 10 different answers.

So let's start with a better question:

What does a business actually need when a cyber incident happens?

The answer isn't just money.

- ✓ **It's expertise**
- ✓ **It's support**
- ✓ **It's a plan**

Cyber insurance is more than a policy

Modern cyber insurance combines three things:

Prevention: Helping businesses identify and reduce cyber risk before an incident occurs.

Response: Providing access to specialist support when something goes wrong.

Recovery: Helping businesses deal with the financial and operational impact of an incident.

Cyber insurance isn't just for after a breach

A modern cyber policy often includes practical support designed to help businesses strengthen cyber security **before** anything goes wrong. This may include:

- ✓ **Awareness training:** Helping staff recognise common cyber threats.
- ✓ **Risk visibility:** Helping businesses understand where vulnerabilities may exist.
- ✓ **Threat alerts and intelligence:** Providing awareness of emerging risks and vulnerabilities.
- ✓ **Access to cyber expertise:** Specialist guidance on Cyber security, resilience and preparedness.
- ✓ **Incident planning:** Helping businesses understand how they would respond if the worst happened.
- ✓ **Outside-in security scanning:** Monitoring of internet-facing systems to identify emerging threats and exposures.
- ✓ **Discounted cyber security services**: Access to trusted cyber security tools and services at preferential rates.

Think of cyber insurance as a team of first responders

They can include specialists who can help to:

- Investigate what happened
- Contain the incident
- Restore systems
- Manage legal obligations
- Communicate with customers and stakeholders
- Handle claims and recovery

Understanding First-Party and Third-Party Cover

One of the unique features of cyber insurance is that it can respond to both the insured's losses and claims brought by others.

First-party cover



First-party cover focuses on the direct impact a cyber incident has on the insured business itself.

These are often the costs that arise immediately after an incident, such as:

- Investigating what happened
- Containing and managing the incident
- Restoring systems and data
- Recovering from business interruption
- Managing extortion demands
- Recovering from cybercrime and fraud losses

In simple terms:

First-party cover helps your client recover from the incident itself.

Third-party cover



Third-party cover focuses on the business's legal liability to others.

This may arise where customers, employees, suppliers, regulators or other third parties suffer loss following a cyber event. Examples can include:

- Privacy claims following a data breach
- Regulatory investigations
- Defence costs
- Settlements and damages
- Claims arising from network security failures

In simple terms:

Third-party cover helps protect the business when others allege they have suffered loss because of the incident.

How the cover applies in practice

All of the examples below could occur following just one incident and yet trigger multiple sections of the policy.

If this happens...	Businesses may need help with...	Typical cover section*	First Party / Third Party
Systems become unavailable	Downtime, extra costs and operational disruption	**Business Interruption**	First Party
Data is lost (exposed), damaged or encrypted	Recovery of systems and information	**System Restoration & Data Recovery and Privacy Liability**	First Party
A cyberattack occurs	Understanding what happened and containing the incident	**Incident Response Services**	First Party
Sensitive information is exposed	Investigation, notifications and specialist advice	**Incident Response Services, Notification Services, Privacy Liability**	First & Third Party
Customers or employees bring claims after a breach	Defence costs, settlements and legal support	**Privacy Liability**	Third Party
A regulator investigates following a breach	Regulatory enquiries and legal representation	**Regulatory Investigation & Fines**	First Party
Money is transferred to criminals	Recovery efforts and financial loss	**Cybercrime & Funds Transfer Fraud**	First Party
Criminals demand payment or threaten to release data	Negotiation support and specialist advice	**Cyber Extortion**	First Party
Malware from the insured's systems affects others	Third-party claims and defence costs	**Privacy Liability**	Third Party
A critical supplier suffers a cyber incident	Loss of service and operational disruption	**Dependent Business Interruption / Supplier Outage**	First Party
Website or systems are used to attack others	Defence costs and damages	**Privacy Liability**	Third Party
The business doesn't know what to do next	Coordination and specialist support	**Incident Response Services**	First Party

*The exact title of each coverage section will vary by insurer and wording. The examples above are intended as generic illustrations of how cyber policies are commonly structured.

Support before, during and after the conversation

You may need support when a client asks about underwriting requirements, existing controls, incident response, supplier risk or how a policy would respond in practice. Those conversations can be complex, and they do not need to happen in isolation.

Brit's cyber proposition is built around access to people with specialist experience across underwriting, claims, breach response and risk management. That means you can start cyber conversations with more confidence, knowing there is practical support behind you when a client question needs a more detailed response.

Key takeaway



Cyber insurance combines prevention, response and recovery.

It can help clients strengthen their resilience before an incident, provide access to specialist expertise when something goes wrong and support their financial and operational recovery afterwards.

First-party cover helps the client recover from its own losses. Third-party cover helps protect the business when customers, employees, regulators or others allege they have suffered loss.

Cyber insurance is therefore more than financial reimbursement. It gives clients access to the people, services and support they may need before, during and after an incident.

Want to explore this further?

Visit the Cyber Knowledge Hub:

Overcoming Barriers to Buying Cyber Insurance for SMEs
Explains why cyber insurance is about far more than recovering from a breach.

Breach Response: Leave It to the Experts
Introduces the specialist support available during a cyber incident.

Digital Forensics: Managing an Online Crime Scene
Explains how forensic experts investigate incidents and help organisations understand what happened.

Ransomware Negotiation: Don't Try This at Home
Shows why specialist expertise is often needed during complex cyber incidents.