

## CYBER LIABILITY AND PROFESSIONAL INDEMNITY

*Reviewed by Matthew Bartlett, Director · Last reviewed 2026-06-23*

---

Cyber liability and professional indemnity are increasingly intertwined for UK professional services firms. A data breach affecting client information is both a cyber event AND a potential PI breach (loss of confidentiality, negligent data handling). Where one policy responds and where the other does is no longer obvious. This entry sets out the practical position.

### HOW THE TWO POLICIES DIFFER

**Professional indemnity** responds to financial loss suffered by a third party as a result of negligent professional advice or services. Coverage is "claims made" — the policy in force when the claim is made responds.

**Cyber liability** is a much broader bundle covering:

- Data breach response costs (forensics, regulator notification, customer notification, credit monitoring)
- Third-party liability for data breach (privacy claims, GDPR-related)
- Ransomware payments (subject to legal restrictions and policy conditions)
- Business interruption from cyber events
- Cyber crime (funds transfer fraud, social engineering — usually sub-limited)
- Network restoration costs

### THE OVERLAP ZONES

Three scenarios where both policies could potentially respond:

1. **Breach of client confidentiality via cyber event.** A professional firm's email is compromised; client documents are exfiltrated. The client sues for breach of confidentiality. Is this PI (loss of confidentiality is a standard PI cover) or cyber (data breach response is a standard cyber cover)?
2. **Professional advice consequent on a cyber attack.** An IT consultant advises a client on security configuration; the configuration is breached; the client suffers loss. The cause is cyber but the trigger is the consultant's advice — squarely in PI territory.
3. **Negligent handling of client data.** An accountant emails client tax returns to the wrong recipient. The client suffers loss and brings claim. Is it negligence (PI) or data breach (cyber)?

### HOW MODERN WORDINGS HANDLE THE OVERLAP

The market has split:

- **Older PI wordings** tend to cover cyber-related claims that arise from "negligent professional advice or services". The professional advice element is the hook.
- **Newer PI wordings** increasingly EXCLUDE cyber events and route them to standalone cyber cover. The exclusion may be narrow (only "cyber attacks") or broad (any "cyber act").
- **Cyber wordings** respond to data breaches regardless of professional advice content. Some cyber wordings exclude professional negligence; some include it.

The result: where a claim could fall under either, the two insurers may dispute who picks up the bill. Best practice: place PI and cyber with the same insurer where possible, or use brokers who can coordinate response.

#### WHAT TO CHECK ON YOUR PI WORDING

1. Is there a "cyber act" exclusion? If yes, how is "cyber act" defined?
2. Is breach of confidentiality covered? Most PI wordings do cover this.
3. Are GDPR-related regulatory investigation costs covered, or routed to cyber?
4. What is the position if a cyber event causes the professional services failure (e.g. ransomware locks the consultant out of client deliverables)?

#### WHAT TO CHECK ON YOUR CYBER WORDING

1. Is professional negligence excluded? If yes, the PI policy needs to be the route for any client-loss claim.
2. What is the data breach notification cover sub-limit?
3. Are ransomware payments covered, and under what conditions (mandatory law enforcement involvement, etc.)?
4. What is the cover position for social engineering / phishing-induced funds transfers?
5. Is there cover for ICO investigation costs? Sub-limit?

#### COORDINATING PI + CYBER

The clean structure:

- **Cyber as primary for cyber-event triggers.** Data breach, ransomware, business interruption — cyber responds first.
- **PI as primary for negligence triggers.** Professional advice or services failure — PI responds first.
- **One insurer or coordinated brokerage** for both, so the response is unified.

Where this matters most: a single event that triggers both policies. The two insurers each want the other to pay. Without coordinated brokerage, the policyholder ends up in the middle.

#### 2026 MARKET POSITION

UK cyber insurance has hardened materially in 2024–25 with mandatory MFA, EDR (endpoint detection and response), backup-segregation requirements, and increased premium. Cyber capacity is constrained for higher-risk industries (professional services firms holding large data sets are higher-risk). PI hasn't seen the same hardening on the cyber side specifically — but PI insurers increasingly exclude cyber acts.

Practically: most UK professional firms now carry standalone cyber alongside PI. The two together cost more than PI alone but less than the alternatives if a cyber claim arrives uninsured.

#### ABOUT APEX INSURANCE BROKERS

Apex Insurance Brokers Limited places PI and cyber liability cover for UK professional services firms. FCA firm reference number 724952. We coordinate the placement so the wordings work together rather than against each other, and explain the boundary where each policy responds.

---

#### RELATED PROFESSIONAL INDEMNITY GUIDES

- [It PI](#)

