THE IT PROFESSIONAL CLAIMS LANDSCAPE IN 2023

10 tips to help IT professionals and their brokers

By Stephen Morrissey
Special Counsel, Wotton + Kearney

As we move into 2023, it appears claims against IT professionals following cyber events are following last year's trend and continuing to increase. Although these claims arise in several ways, managed services providers (MSPs) and cloud services providers (CSPs) that are responsible for hosting the data of their clients continue to be common targets for cyber criminals. The pressure these IT professionals face from their clients to resolve the cyber incident (i.e. pay the ransom) often provides significant leverage in favour of the cyber criminals.

While MSPs and CSPs are not always the direct victims of a cyber incident, they can often be blamed when a client suffers a cyberattack. These allegations typically involve arguments that the MSP or CSP was responsible for the client's cyber security posture and/or backup management, which can be crucial in minimising the impact of a cyber incident.

TYPICAL CLAIMS

Claims against IT professionals are typically founded on an allegation that:

- the MSP/CSP did not have adequate cybersecurity measures in place to prevent attacks against it in the case of direct cyberattacks against MSPs / CSPs, or
- the IT professional did not implement or recommend adequate cybersecurity measures in the case of cyberattacks against clients of IT professionals.

The claims are typically framed in negligence, breach of contract and/or breaches of consumer law, such as misleading or deceptive conduct or consumer guarantees. Affected clients typically seek compensation for the costs of responding to the incident, reconstituting and/or recovering their data, and business interruption.

We offer 10 tips to help IT professionals (with the assistance of their brokers) avoid being exposed to these type of claims and the associated legal defence costs.

wotton kearney

Tip #1 – Get the contract right
In any contract imposing an obligation on the IT professional to provide, or advise on, cybersecurity, it is important to clearly define responsibilities and avoid any ambiguity. This should include specifying the obligations and limitations of the IT professional's services, identifying any aspects of the client's cybersecurity that are not the responsibility of the IT professional, and bringing any relevant terms and conditions (e.g. limitation of liability clauses) to the client's attention.

It's worth noting many insurers offer a limited number of contract reviews per policy year.

Tip #2 – Be careful and skilful
To state the obvious, if an IT professional is responsible for cybersecurity, they should exercise due care and skill in providing their services. That will likely include identifying, documenting and communicating any cybersecurity vulnerabilities, and ensuring that they do everything within their power (e.g. patching) to reduce the risk profile in line with their contractual obligations.

Tip #3 – Document all client conversations
IT professionals should document any recommendations or warnings they provide to clients around cybersecurity, to support any potential future argument regarding whether they properly discharged their obligations.

Tip #4 – Check automated security and retention processes
IT professionals should regularly check that automated security or retention processes are working as intended. It only takes one instance of failure to create a claim risk.

Tip #5 – Don't rely on the limitation of liability clause
Often limitation of liability clauses are not the lifesaver that IT professionals expect. They can be vulnerable to the operation of the unfair contract terms regime in the Australian Consumer Law as liability clauses usually don't apply to consumer law allegations, such as misleading or deceptive conduct.

Tip #6 – Respond proactively to an incident
IT professionals should consider third party claims mitigation during the incident response phases following a cyberattack. If an IT professional takes proactive steps to support its clients following an incident, experience tells us that this can significantly reduce claim risk.

Tip #7 – Take other mitigation steps
IT professionals should also consider taking other mitigation steps, including forensic investigations that focus equally on how clients have been impacted, as well as planned and periodic client communications in the immediate aftermath of an incident.

Tip #8 – Say no
If cybersecurity is not within an IT professional's expertise, they should not pretend that it is. Only bad things can happen from doing so.

Tip #9 – Contact the broker and insurer quickly
It is important that IT professionals contact their broker as soon as they become aware of an incident. Brokers can assist in notifying the insurer and advising on the next steps.

Tip #10 – Plan for the worst
Wotton + Kearney regularly assists brokers and their IT professional clients with risk mitigation strategies and breach management plans. These are designed to put IT providers in the best position possible to manage risks, guard against cybercrime and respond to third party claims.