# Ten ways IT professionals can avoid the blame game after a cyber breach

SEPTEMBER 2022

Australia is suffering from a ransomware 'epidemic'. In recent times, there has been a major increase in the frequency of claims, the scale of demands, the size of ransoms paid and the frequency of multi-party incidents. Often, these attacks also involve 'double extortion', as theft of data now accounts for 86% of incidents.

Given the volume of incidents, it's not surprising that IT providers are increasingly being affected by both platform/supply chain and direct attacks.

Platform/supply chain attacks involve threat actors exploiting the software supply chain process, supplier trust and open source vulnerabilities. They achieve large-scale impact with multiple victims through a single initial compromise that creates a snowball effect.

IT providers (in particular managed services providers) are also an attractive target for direct attacks given the potential knock-on impact to their clients and a likely increased motivation to pay the ransom.

These attacks are increasingly leaving IT providers at risk of claims made by clients who are victims of the breach. Claims can arise from allegations of negligence/duty of care, breach of contract or breaches of consumer law, such as misleading/deceptive conduct or consumer guarantees.

To avoid becoming the legal scapegoat following a direct or indirect cyber breach, there are 10 ways IT providers can help protect their positions:

## 1) Get the contract right

In any contract involving cybersecurity, it is important to clearly define responsibilities and remove/avoid ambiguity.

Securing a network is a multi-layered responsibility that includes both organisational capabilities (e.g. skilled people, an incident response plan and security scans) and technical capabilities (e.g. anti-malware systems and centralised logging).

Responsibilities for cybersecurity between an IT provider and its client should be clearly documented in contracts and SLAs that are commonly understood by all parties. This includes specifying the obligations and limitations of the IT provider's services, scoping out any areas of cybersecurity that are not the responsibility of the IT provider, and clarifying the terms and conditions. When the terms and conditions need to be updated, this should be done quickly and directly with the client to provide certainty for future dealings.

## 2) Be careful and skilful

If an IT provider is contractually responsible for any aspects of cybersecurity, they should approach their obligation with due care and skill. This is likely to include documenting and communicating security weaknesses with the client to ensure a common understanding of the risk profile.

Even if an IT provider is not contractually responsible for any aspects of cybersecurity, it should still consider raising security issues with its clients.

## 3) Document all client conversations

It is useful to provide warnings and recommendations to clients that are designed to prevent breaches. It is equally useful (if not even more so) to keep records of these communications. In many cases, disputes can turn on contested, undocumented conversations which (if proven) would otherwise demonstrate the IT provider had met their obligations. Accordingly, it is important to make and keep file notes or confirm client discussions in writing.

## 4) Check automated security and retention processes

If automated security or retention processes are in place, IT providers should check on a regular basis that these are working as intended – without exception. It only takes the one instance of failure to create a liability and claim risk.

## 5) Contact the broker or insurer quickly

It is important for IT providers to notify their broker or insurer as soon as a breach occurs. It is also important that they inform the insurer of letters alleging breaches or errors – and never ignore them.

## 6) Don't rely on the limitation of liability clause

Often limitation of liability clauses are not the lifesaver most businesses expect. This is because the clauses are potentially void under unfair contract terms legislation. They also typically don't apply to consumer law allegations, such as misleading or deceptive conduct.

## 7) Take positive steps to support the client after a breach

A better approach is for IT providers to consider third party claims mitigation during the incident response phase following a cyberattack. When an IT provider takes positive steps to support the company following a breach, this significantly reduces the possibility of action being taken against the IT provider. In many cases, proactive support strengthens the relationship between the IT provider and their client.

## 8) Take other mitigation steps

Other mitigation steps can include ensuring that forensic investigations focus equally on ascertaining how clients and the insured have been impacted.

While planned and periodic communication is also key, IT providers should be careful not to admit liability.

## 9) Say no

One of the best ways to limit the risk of claims is to 'stick to your knitting'. In other words, if cybersecurity is not within an IT provider's skillset, they should decline to take the work. Similarly, they should say "no" to clients that do not fit their business model.

## 10) Plan for the worst...

Wotton + Kearney can assist with privacy and security risk mitigation strategies and breach management plans. These are designed to put IT providers in the best position to manage risks by helping them meet privacy regulation and notification obligations, address commercial and IP data loss issues, guard against cyber extortion and cybercrime, and respond to regulatory investigations and third party claims.

Authors: **Kieran Doyle** (Partner, Head of Cyber + Technology), **Stephen Morrissey** (Special Counsel)





wotton kearney

# Need to know more?

For more information, contact one of our senior **Technology Liability** specialists.


**Kieran Doyle**
Head of Cyber + Technology, Sydney
T: +61 2 8273 9828
kieran.doyle
@wottonkearney.com.au

**Joseph Fitzgerald**
New Zealand Cyber Leader, Wellington
T: +64 4 260 4796
joseph.fitzgerald
@wottonkearney.com.au

**Nick Lux**
Partner, Melbourne
T: +61 3 9604 7902
nick.lux
@wottonkearney.com.au

**Stephen Morrissey**
Special Counsel, Sydney
T: +61 2 8273 9817
stephen.morrissey
@wottonkearney.com.au

**Magdalena Blanch-de Wilt**
Special Counsel, Melbourne
T: +61 3 9116 7843
magdalena.blanch-dewilt
@wottonkearney.com.au