EMERGENCE INSURANCE

emergence

cyber insurance objection handling

Emergence is your award-winning underwriting agency focused on providing flexible, innovative insurance solutions to help protect businesses against cyber risks.

When it comes to handling objections by your clients when offering cyber insurance, confidence is key. Many SMEs have misconceptions, cost concerns, or a lack of awareness about cyber risks. This guide provides clear responses to common objections, helping you educate your clients and highlighting the critical role of cyber insurance.

“My business is too small to be targeted”

Highlight vulnerabilities

Threat actors are not necessarily targeting big or small businesses, rather they attack businesses that have poor IT security and hygiene. With SMEs often not having the same cyber security defences in place as large corporations, they are an easier target.

Paint a picture of how attacks are executed

Financially motivated threat actors rarely target individual businesses. They rely on automated attacks. These threat actors launch phishing campaigns to exploit individuals into clicking malicious links or downloading infected attachments, thereby gaining unauthorised access to business systems. Once they gain access, they can encrypt business files, demanding a ransom for their release, alter invoices, or send phishing emails to clients.

Position cyber insurance as a business continuity tool

Think of cyber insurance like property insurance. Think ‘Digital Fire™. You may never have a fire, but would you risk operating without property insurance? A cyber event can disrupt your business just as much as a fire can, resulting in business interruption and financial losses.

VULNERABILITIES

Use claims examples to show how vulnerable small businesses are.

CYBER TACTICS

Educate on how cyber attacks are actually executed.

CYBER RISK

Compare cyber risk to traditional business risk.

EMERGENCE INSURANCE

emergence

cyber insurance objection handling

“My IT Provider / Managed Service Provider has this covered”

Explain the limits of their responsibilities
An IT providers role is system and network management, not financial risk protection. IT providers might help prevent attacks, but they don’t cover financial losses, reputational damage, or legal fees when a breach occurs. If hackers steal your client data or hold your systems for ransom, your IT provider will often not pay for data recovery or legal costs. Cyber insurance will.

Highlight third-party risk exposure
Even if your IT provider is secure, what if a vendor or supplier you rely on suffers a cyber event? Cyber insurance can cover business interruption and liability costs if your operations are affected by a cyber attack.

Question incident response capability
Your IT provider may not be an incident response expert. While they may assist with system recovery, who will handle crisis communications, regulatory obligations and digital forensics work to recover data or negotiate ransoms?

IT PROVIDER FAILED

Show an example where an IT provider failed to prevent an attack.

SYSTEM V FINANCIAL PROTECTION

Explain the difference between system and network management services and financial protection.

REVIEW IT CONTRACT FOR GAPS

Ask the Insured to review any potential cyber gaps or limits of liability in IT provider contracts.

EMERGENCE INSURANCE

emergence

cyber insurance objection handling

“Our data is secure in the cloud”

Cloud providers secure their infrastructure, but businesses must protect their own access and data. Breaches happen, but through compromised credentials, logins, and passwords. Whether using cloud storage, web-based email, or other third party platforms, stolen credentials remain a leading cause of cloud-based breaches.*

*2025 Verizon Data Breach Investigations Report (DBIR).

“Cyber insurance is too expensive”

Compare the cost of insurance to the financial impact of an incident. What about business interruption cost? 60% of SMEs don’t survive a cyber attack.*

*The Australian Small Business and Family Enterprise Ombudsman, 2023.

“We have cybersecurity measures in place, we are safe”

No system is 100% secure, and human error is the one of the biggest risk factors. In 2024, human error caused 30% of data breaches.* Multi-layered security helps, but attacks still happen (e.g., social engineering, credential theft).

*OAIC Notifiable Data Breaches Report January 2024.

“We don’t rely on technology”

Even businesses with minimal technology still use email, banking systems, and customer databases. If your critical systems went down, how long could you operate? What would the impact be on revenue and customer trust?