

Cyber

A solid blue horizontal bar.

Over the past year, we've seen some notable shifts in the cyber insurance market. First, the market is showing signs of softening. Second, coverage continues to evolve. And third, the threat landscape and regulatory environment are shifting together.

Beginning with the market itself showing signs of softening – in the first half of 2025, common market sentiment pointed to plentiful capacity and strong competition, with premium reductions common and, in some cases, savings being reinvested into additional cover – reinforcing the impression of a market under competitive pressure. That mirrors the global experience, where premiums have been easing over the past two to three years, following the earlier period of sharp increases in response to ransomware.

Next, we're seeing coverage continue to evolve alongside the risk environment. With competition increasing, insurers are broadening terms and often providing free add-ons or riders. A portion of the market is throwing in dependent business interruption (or DBI) at no extra cost, or extending policies in Australia to cover property damage and bodily injury, as we've seen with Coalition. There are also new offerings targeting SMEs, such as Ocean Underwriting's tailored cyber cover for SMEs, and Upcover's self-service cyber product launched in August. It's worth noting that DBI also carries the potential for catastrophic scenarios, given the concentration of reliance on common providers like AWS or Azure. A single outage there could impact thousands of insureds simultaneously. Something to watch out for!

Finally, the threat landscape and regulatory environment are shifting together. Attackers are increasingly targeting managed service providers and critical suppliers, creating systemic exposures and amplifying claim severity. Regulators have taken note. APRA's 2025–26 corporate plan prioritises compliance with the new CPS 230 operational risk standard, and ASIC has stepped up enforcement, with two cyber-related proceedings already this year, most recently against Fortnum Private Wealth in July. These developments reinforce that boards and executives are expected to treat cyber resilience as a governance priority.

So, to sum up: as a cyber insurer in a softening market, you'll need to balance sharper competition with underwriting discipline by differentiating through innovative coverage and services, tightly managing systemic risks from dependent providers and supply chains, and positioning yourself as a resilient, trusted partner to clients and regulators.