Cyber Insurance - Once More Unto the Breach

TOP 5 TIPS

The cyber market has seen some recent instability. A wave of cyber events (particularly Ransomware) drove harder market conditions and the raising of the bar on cyber security requirements. This has attracted new insurers and competition is intensifying again. However, the underlying themes haven't changed and remain vitally important. Here is a quick reminder:

1. Underwriting the Risk

Cyber is no different from other insurance products and it is fair to assume that better risk mitigation will lead to improved terms, but that is not always the case. Positively answering questions can help find cyber cover, but wordings may still contain specific security requirements.

Further questions and analysis will identify those risks with a stronger security posture and help secure more favourable terms.

2. Incident Response

Wordings have become increasingly standardised as the cyber market has evolved, but the crucial incident response services can still differ significantly and need to be thoroughly examined.

Incident response should be pro-active, with the ability to scale resources quickly. Time is vital during a cyber event and it is much easier to stand down a comprehensive response than it is to raise an inadequate one.

Using a specialist incident response provider (rather than an in-house claims team) can often be more favourable as it separates the insurer consideration from the process.

3. A Strong Product

Cyber wordings have evolved over time and have become easier to compare, but significant differences still exist. An obvious one is the requirement to adhere to security requirements (often a feature of streamlined underwriting methods).

Trusted products that have been tested should have an advantage, particularly those without the onerous requirements.

Insurers that offer primary and excess layer options can provide additional flexibility, especially on more complex risks or those with higher limit requirements.

4. Crime Cover

This remains a key area as exposures overlap, and it can be difficult to determine the correct home for Cyber Crime.

Cyber Insurance was designed to protect organisations from some aspects of criminal activity (such as data breaches or extortion) whereas Crime Insurance generally focussed on protecting organisations in relation to theft and fraud, so it is easy to see how these exposures have become tangled, particularly in relation to social engineering fraud.

As cyber insurers limit the crime cover, it is helpful to have an insurer that can help navigate the exposures and offer a standalone Crime product if required.

5. Communication with the Regulator

This goes hand-in-hand with the quality of incident response and the speed/proactivity required in handling a cyber event.

The situation must be expertly assessed to establish any ICO notification requirement. If that is required, clear and concise information exchange is vital. Within 72 hours of an event occurring there may be a need to explain what happened, how existing defences were breached and what measures have been taken to mitigate.

Having legal input available for that immediate incident response service is incredibly useful, not only in terms of legal privilege but also in understanding and navigating the regulatory process.

MPR | MANAGEMENT & PROFESSIONAL RISKS

To be solid, insurance must be flexible