MPR | MANAGEMENT & PROFESSIONAL RISKS

Accessing Cyber Insurance & the Importance of Incident Response

In 2017, I wrote an article titled Cyber events and the importance of incident response. A lot has happened since, so it seemed like an appropriate time to sense check the different approaches to underwriting Cyber Insurance that have developed. In those seven years we have seen changing market cycles, insurer instability, new products and evolving complimentary services, with a lot of turbulence and much to reflect on.

$33.4 billion

Global cyber insurance market is forecast to grow from $16.7 billion in written premiums in 2022 to $33.4 billion in 2027 (GlobalData – 2023)

Cyber comes down to simple risk transfer. A client will seek to minimise the risk initially by incorporating a good cyber security posture into their systems and operations. Then, if necessary, they might choose to transfer the balance of risk via an insurance policy. Insurers will provide the policy based on analysis of the risk and existing mitigation in place. It sounds simple, but the cyber underwriting process has been volatile in recent years and has only recently settled into three typical patterns:

1) Quick, cheap and cheerful:

A policy is purchased in a simplified way with a basic risk-mitigation question set or a statement of fact, facilitating a swift quote and bind process. It's the easiest path to purchase and often favoured in the SME space. There is minimal opportunity for a buyer to differentiate risk and influence premium and cover (other than through size & industry sector) and negligible interaction with an underwriter. Often, this policy is likely to provide entry-level cover and/or may contain requirements for the buyer to maintain certain standards of cyber security. This might be stated in the application language or built in to the policy coverage. Provided all of that is communicated clearly, it remains a simple, effective way to obtain Cyber Insurance.

> "We want to see a cyber insurance market where firms can demonstrate that customers buy products that meet their needs and provide value, to avoid misalignment between customer expectations and policy outcome. Firms offering cyber insurance must make sure their policy wordings are clear and that customers understand the coverage they are buying. We also expect firms to manage cyber claims handling in a fair and timely way... We will continue monitoring the cyber insurance market and take action on firms we deem to be outliers."
>
> FCA - Insurance Market Priorities Letter 2023-2025 (20/09/2023)

2) Open source intelligence and cyber insurance 'as a service':

A policy is purchased with broader risk management questions in a relatively streamlined fashion and without the need for security requirements to be built in to the policy. Some buyer differentiation can be achieved with positive question responses, but the pricing remains fairly standardised and largely governed by size and sector. Underwriter interaction remains low-touch with part of the risk transfer process achieved by insurers incorporating open source intelligence ('OSINT') to 'pre-screen' and evaluate their potential customers. This is achieved primarily through assessing vulnerabilities in their website/web-applications. It is a completely legal process (information is gleaned solely from public sources) and can be a good tool for spotting threats, especially as cybercriminals use similar methods to plan for a cyberattack. This service often extends to continuous monitoring during the policy period, advising customers on CVE's (latest publicly known 'common vulnerabilities & exposures'). It has become an attractive proposition in recent years, particularly for customers who prefer some assistance or guidance in cyber security. However, larger clients with experienced IT teams can sometimes find the interference frustrating and the regular security updates can even create a level of 'alert-fatigue'. It's also been argued that OSINT, whilst a useful assessment tool, doesn't always give a true reflection of the overall risk mitigation of a customer. There is also the question of how the insurance policy will respond if a mid-term security alert is not acted upon.

3) Higher touch, engaged underwriting:

A policy is purchased with a more detailed underwriting process in a higher-touch approach where engagement is encouraged between customer, broker and underwriter. This may involve further risk information gathering and additional questions, but allows articulation and differentiation of risk in more detail, moving away from the one-size-fits-all approach. Premium is not solely determined by generic rates, but by a bespoke process with further discounts often offered due to enhanced understanding of the risk mitigation. OSINT can be used as part of the pre-bind engagement but assessed in conjunction with overall risk information to ensure that the broader cyber-security posture is understood. Constant monitoring and alerts throughout a policy period are not required by the insurance provider as the bespoke process ensures both parties are fully comfortable at the bind stage. For larger risks, the level of engagement can extend to pre or post-bind calls to introduce incident response providers and create stronger relationships. This can also facilitate updated incident response plans or provide flexibility to include the insureds existing cyber security providers into the incident response process. This method is generally suited to larger and/or more complex risks, but is also heavily influenced by accessibility to underwriters.

Regardless of which path is taken to purchase a cyber policy, one of the most important decisions should centre on the incident response process, i.e. what actually happens when a cyber event occurs? It is here that the devil really is in the detail.

The first hours following a cyber event are crucial. This is where the incident response and subsequent decisions can have the biggest impact on any organisation. A quality incident response provider should offer a 24/7/365 service and ability to engage a collaborative Crisis Management Team swiftly.

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. A good insurer will view high quality incident response services as mutually beneficial and may even offer a zero excess for the initial triage stage to ensure there is no hesitation in response. This is on the basis that speed and quality will minimise the impact to the insured and therefore reduce the severity of claim for the insurer.

Using a specialist incident response provider (rather than an in-house claims team) can often be favourable as it separates the insurer consideration from the process, allowing the incident response team to work swiftly in conjunction with the client for their best outcome, not the insurers. Likewise, 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 and assessing any ICO communication/notification requirements.

> "We provide round the clock access to fully qualified lawyers with significant experience in dealing with cyber breaches. This early introduction of lawyers allows legal privilege to the fullest extent possible and helps to ensure key legal and regulatory deadlines are identified upfront"
>
> – RPC ReSecure

When it comes to incident response, there is no substitute for experience and those providers established for many years will have dealt with many cyber events and are more likely to possess the knowledge and confidence to help an insured in their time of need

> "The ReSecure team was the first and remains one of the few 'full-suite' cyber incident response services for insured clients, established in the UK 12 years ago. Prior to that the STORM team members were responding to incidents for an additional twenty years. With the total number we have handled in the thousands, there is not much we haven't seen when it comes to cyber claims"
>
> – Storm Guidance (part of the ReSecure Service)

So, whilst there has been a great deal of change in the Cyber Insurance market in the last in seven years, the same key concepts remain vitally important and should always be examined as part of the purchase. Having a healthy and competitive market with different approaches not only gives brokers the choice of what is best for their clients' needs but will also bring out the best in products and service.

Want to find out more?

Call: 0161 241 3550
Email: enquries@mprunderwriting.com

Visit our website to find out more about our products and to keep up to date with the latest financial lines insights.
www.mprunderwriting.com