2024 Cyber-insurance

Market Outlook

Increased cyber-attacks with new evasive tactics, hacktivist-based attacks and frequent ransomware have created a volatile risk environment for organisations of all types and sizes over the past few years. The increased cost of dealing with such disruptive incidents created a hard market, with most policyholders facing premium hikes. Indeed, cyber-insurance pricing rose a staggering 66% in the UK in the third quarter of 2022, according to insurance broking and risk management company Marsh.

Fortunately, Marsh's latest report describes an improved position. Specifically, increased market competition and healthier insurer loss ratios have had a moderating impact on pricing, and the market has displayed indications of softening during 2023. In fact, cyber-insurance premiums moderated to 11% in the second quarter last year, and prices may continue to stabilise in 2024. However, rising geopolitical tensions and a continually evolving cyber-landscape make accurate pricing predictions difficult. Therefore, organisations should adopt a strong security posture and stay abreast of market developments.

Developments and Trends to Watch

- **Ransomware:** Ransomware remains a top risk for organisations as ransomware groups continue developing tactics and operating at larger scales. A new tactic emerged in 2023 whereby cyber-criminals target third-party software to compromise the data of several organisations simultaneously, as demonstrated by the MOVEit data breach in May 2023. As such, robust cyber-security measures relating to ransomware and supply chain perils are critical for risk management endeavours and may also be required by insurance carriers to qualify for policies or reduced premiums.
- **Artificial intelligence (AI):** AI-driven cyber-threats continue to grow as 2024 begins. Although AI tools can help organisations detect and neutralise threats and automate incident response, they can also be weaponised by cyber-criminals. For instance, generative AI has begun to aid the phishing market, with AI tools able to formulate sophisticated phishing messages, including convincing deepfake attacks, with minimal effort. Organisations should understand both the risks and advantages of AI to help combat losses.
- **Business email compromise:** Business email compromise (BEC) occurs when a cyber-criminal impersonates a legitimate source via email (eg a senior manager, business partner or vendor). Threat actors use these emails to gain the trust of their targets to trick them into transferring money, sharing sensitive information or engaging in other compromising activities. As remote and hybrid working patterns increase, email systems are a desirable target for criminals. As such, organisations should understand the types of BEC scams and check their policies, including cover for BEC fraud.
- **Policy terms and cyber-security regulations:** As the government implements measures to protect national security from cyber-attacks—especially cyber-warfare—new regulations may develop. For instance, UK businesses have until April 2024 to comply with the Product Security and Telecommunications Act, which requires manufacturers of connected products to abide by minimum security standards. Organisations must comply with all legislation to keep risks at an acceptable level. Additionally, policyholders should scrutinise policy terms and conditions as many insurers now exclude certain lines of cover (eg cyber losses arising from war).

Tips for Insurance Buyers

- Work with your insurance professionals to understand the different types of cyber-cover available and secure a policy that suits your unique needs. Carefully examine policy terms and conditions and any exclusions.
- Consider robust employee training to prevent cyber-crime from affecting your operations. Include any pertinent cyber-threats—especially AI-powered attacks, ransomware and BEC scams—in your teachings. However, avoid just asking employees to attend frequent awareness training, as this can lead to security fatigue. Instead, consider ways to make cyber-security an integral part of company culture.
- Establish a cyber-incident response plan to build cyber-resilience and minimise damages in the event of a data breach or cyber-attack.
- Consult insurance and legal professionals to determine your organisation's regulatory exposures regarding applicable data protection and cyber-security regulations. Make compliance adjustments as needed.