2023 Cyber Insurance

Market Outlook

Cyber-attacks continue to occur frequently across industry lines, with nearly 1 in 4 (24%) IT professionals reporting that their organisation fell victim to a ransomware attack in 2022, according to cloud email security provider Hornetsecurity. This increase in cyber-crime has contributed to a hardened cyber-insurance market, as the cost of dealing with these incidents helped drive insurance costs up. Indeed, global cyber-insurance pricing rose 53% in the third quarter of 2022, according to insurance broking and risk management company Marsh; in the UK alone, prices for cyber-cover rose 66% during that period. While prices seem to be rising at a slower rate than in previous quarters, the overall market-hardening could persist into 2023 as cyber-threats—and their related costs—continue to evolve. As such, organisations should stay apprised of the following market developments that may affect cyber-insurance premiums or policy terms.

Trends to Watch

- **Deepfake attacks**—A deepfake is an image or video convincingly altered to misrepresent someone. For instance, fraudsters may clone the voice of a company director to trick employees into releasing money or data. Deepfakes are becoming increasingly sophisticated as technology advances. As such, employees may be more likely to fall for deepfake attacks in 2023, so it may be pertinent to cover the topic of deepfakes in employee cyber-training.

- **Internet of Things (IoT) vulnerabilities**—Management consultant company Gartner predicts that 43 billion IoT objects, such as "smart devices" and voice assistants, will be circulating globally in 2023. Unfortunately, many devices have limited built-in security, so they are easy targets for cyber-criminals. Organisations should protect themselves by having employees use strong, unique passwords and regularly update IoT device software.

- **Opportunist attacks**—Opportunist fraudsters could tap into employees' fears to steal money or personal information amid the cost-of-living crisis. For instance, numerous emails related to fraudulent energy rebate offerings were reported to the suspicious email reporting service last year. As the economic downturn persists, so could the trend towards opportunist attacks; this includes the persistent trend of ransomware attacks. Additionally, geopolitical tensions—such as Russian's invasion of Ukraine—will continue to increase global cyber-warfare risk.

- **The rise of artificial intelligence (AI)**—AI tools can examine data in real time and recognise cyber-threat patterns. AI tool use may extend to automated security controls and response mechanisms, helping organisations respond faster to cyber-attacks in 2023. However, as AI responses are based on threat understanding, it's vital that organisations keep up to date with the latest attack methods and trends.

Tips for Insurance Buyers

- Employees are commonly targeted during cyber-attacks, making them your first line of defence. As such, consider ways to make cyber-security an integral part of company culture. Additionally, focus on employee training to prevent cyber-crime from affecting your operations.

- Utilise security services offered by insurance carriers and third-party vendors to strengthen your cyber-security measures. These should include implementing multifactor authentication and keeping devices and software up to date.

- Work with your insurance professionals to understand the types of cyber-cover available and secure a policy that fits your needs. Additionally, discuss cyber-risk mitigation efforts that may help you reduce your organisation's exposure to cyber-crime.