Hanyani Mabaso

Associate Director
Insurance
Tel: +27 82 870 7883
Email: hanyani.mabaso@kpmg.co.za

Are you prepared to tackle cyber-attacks head-on?

Introduction

The insurance industry has evolved alongside the constantly growing economy and has adapted to the complexity that comes with the evolutions in global trade and technology advancements to stay relevant in today's world and respond to present-day risks. Currently, cybersecurity is a growing threat and has become a top priority for executives globally. According to the World Economic Forum Global Risks Perception Survey (2023), cyber-attacks on critical infrastructure ranked fifth in terms of risks that are most likely to present a material crisis on a global scale.

The challenges presented by advanced networks and computer applications in today's world create cybersecurity vulnerabilities even in developed economies. Since the onset of COVID-19, the rise in remote work and data access has kept people connected despite physical barriers. While there are benefits to this increased connectivity, it also comes with cybersecurity risks. The increase in home connectivity, self-driving vehicles and generative artificial intelligence (AI) creates more data points, leading to opportunities for advanced cyber-attacks.

In response to the increasing threat of cyber-attacks, regulators around the world are taking action. In South Africa, the Prudential Authority issued a joint standard on cybersecurity and cyber resilience. This standard outlines the requirements for sound practices and processes related to cybersecurity and cyber resilience for financial institutions operating in South Africa.

The problem statement

In response to the increasing threat of cyber-attacks, insurers are having to evolve the nature of cyber insurance product offerings in line with the changing cyber threat landscape, which includes data breaches and ransomware attacks. Factors such as increasing computing power available to criminals, as well as the commoditisation of cybercrime through ransomware, further propels the opportunity for cyber criminals.

Given that these risks are dynamic and may not be well understood, underwriting may be challenging because of the complexity and uncertainty involved in estimating future losses, and not having sufficient claims history to accurately project claims and assess underwriting risk factors.

The risk of cyber-attacks is a serious concern for insurers and individuals alike. The growing availability of online and digital banking services has provided cyber-criminals with more opportunities to commit online banking fraud. Although banking fraud primarily targets individuals, it can also affect other entities.

There is a great opportunity for insurers in South Africa. Some consumers are aware of the importance of detecting and preventing cyber-attacks, but they will also be turning to the insurance market to help manage the risk in case their preventive measures fail.

KPMG

The opportunity

Munich Re's 2024 Risk and Trends report noted the high proportion of uninsured cyber risks, the growing demand for cyber insurance and that 87% of managers surveyed believe their company is not adequately protected against cyber risks. The increasing threat from cyber criminals is driving the need for cyber insurance across the globe.

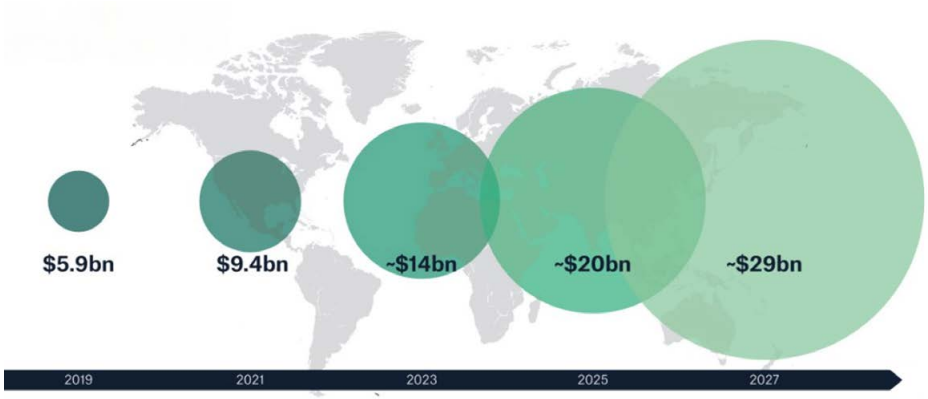
Studies on cybersecurity reveal that organisations are not fully prepared for the growing frequency and complexity of cyber-attacks, including the related potential financial impacts. Many organisations overestimate their ability to deal with these threats and are not accurately assessing the scale of challenges that might materialise.

At the core of an insurance business is the management of risk, and every risk presents an opportunity. Insurance companies in South Africa are encouraged to continue to innovate and offer tailor-made products that address the diverse needs of policyholders relating to cybersecurity, in respect of organisations and individuals alike. This may come at a high cost to the policyholder. Caution should be exercised in underwriting these risks as claims related to cyber-attacks could be substantial, with the availability of court precedents in respect of related claims disputes being limited.

In determining the risks to be underwritten, the insurance company and policyholder will need to align to clearly understand and define the specific risks and circumstances being covered. In addition, the insurer should also ensure that reinsurance structures are appropriately aligned to manage its own capital and solvency requirements.

Conclusion

Cyber insurance market: gross written premium expectations 2019 - 2027



Source: Munich Re: 2024

The cyber insurance market is expected to grow to USD 29 billion by 2027, driven by the awareness of the increasing frequency and sophistication of cyber-attacks and the potential financial repercussions, as well as by stricter regulatory requirements.

The growing threat from cyber criminals and rapid technological advances are fuelling the demand for cyber insurance across the globe. South African insurers should be prepared to develop products that cater to diverse client needs, while at the same time gaining a competitive edge. However, caution should be exercised as this is a relatively new area. Herein lies the opportunity for the insurance industry – to go back to basics and do what it does best, protecting the public interest in times of need.

Reference list:

1 World Economic Forum (2023). Global Risks Report 2023. [online] World Economic Forum. https://www.weforum.org publications/global-risks-report-2023/

2 Financial Sector Regulation Act, 2017 - Joint Communication 6 of 2021 https://www.resbank.co.za/en/home/publications publication-detail-pages/prudential-authority/pa-public-awareness Communication/2024/Joint-Communication-2-of-2024-Publication of-the-Joint-Standard-Cybersecurity-and-cyber-resilience

3 SABRIC. (2021). SABRIC ANNUAL CRIME STATS 2021. [online] https://www.sabric.co.za/media-and-news/press-releases/sabric-annual-crime-stats-2022/

4 www.munichre.com. (n.d.). Cyber Insurance: Risks and Trends 2024 | Munich Re. [online] https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

5 newsroom.cisco.com. (n.d.). 2024 Cisco Cybersecurity Readiness Index. [online] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m03/cybersecurity-readiness-index-2024.html

6 INTERPOL's African Cyberthreat Assessment Report (2023), - Bing. [online] https://www.bing.com/search?pglt=163&q=INTERPOL%E2%80%99s+African+Cyberthreat+Assessment+Report+(2023)%2C&cvid=51de492976084506a1e897f5e672897b&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICAEQ6QcY_FXSAQc4MzFqGoxqAIIsAIB&FORM=ANNAB1&PC=U531