Singapore's cyber focus creates path for (re)insurers

OCTOBER 12 2020 by Yvonne Lau

In Focus Cyber Digital Legal/Regulatory Pandemic Singapore

Singapore has been ramping up measures to pave a secure cyber path for (re)insurers and other financial institutions, with the cybersecurity focus set to increase further in the post-Covid era.

In recent years, the Lion City's cybersecurity regime has shown "increased maturity," Magda Chelly, head of cyber risk consulting for Marsh Asia noted to InsuranceAsia News (IAN). There have been new security acts, amendments to privacy laws and awareness initiatives implemented.

In July, the Monetary Authority of Singapore (MAS) proposed new legislation to expand its oversight on cyber regulation, and an increased penalty for breaches of cyber risk requirements.

This enhanced oversight is set to further the city's cyber regime.

As Karen Lee, Mayer Brown counsel in Singapore, told IAN, the new legislation enables them to "specify technology risk management requirements for financial institutions in any class and in relation to any system — not just for regulated activities as is the current case."

> ***"We have been closely monitoring financial institutions to ensure adequate controls. [This includes] malware updates and security patches to systems and staff devices." MAS spokesperson***

"This new law will complement the existing Cybersecurity Act [effected August 2018], which requires... [compliance] with codes of standards [for] cybersecurity measures," she added.

And with Covid-induced new norms of remote working, the Authority has heightened cyber surveillance and circulated new advisories to (re)insurers ensuring a ramp up of online defenses.

"We have been closely monitoring financial institutions to ensure adequate controls. [This includes] malware updates and security patches to systems and staff devices," a MAS spokesperson noted to IAN.

Enhanced cooperation

Another positive development is that Singapore's market players are committed to working together.

Ronak Shah, the General Insurance Association of Singapore's (GIA) management committee member and market development committee convener (and chief executive QBE Singapore), says public-private collaboration has increased "significantly" in recent years.

> ***2019 was a significant year for cybercrime in Singapore. The city saw a 50% rise, primarily in e-commerce scams, phishing and malware targeted at the financial sector.***

Initiatives by the regulator and insurers work hand-in-hand to boost online protection for SMEs to large corporates, Shah explained. For instance, the GIA is undertaking various cyber

literacy programmes with the expectation that increased awareness will mean the same for expectations for businesses to be "fully equipped in keeping personal data safe."

2019 was a significant year for cybercrime in Singapore — Shah noted the city saw a 50% rise, primarily in e-commerce scams, phishing and malware targeted at the financial sector.

Meanwhile 2020 has seen a spike in inquiries and potential demand for cyber risk products, in part due to the pandemic.

For (re)insurers, these developments call for a response in offerings and strategy. Shah advises carriers to work with companies to introduce relevant new initiatives and products "beyond just issuing a one-time claims payout."

Ali Chaudhry, Marsh Asia's finpro leader, added: "The increasing use and integration of technology into all aspects of our lives will drive cyber insurance demands — especially if existing conventional insurance products and their providers are unable to evolve their products to these new relevant and evolving perils."

Post-pandemic path

For all of Asia's digital interconnectedness, it is vastly under protected when it comes to cyber risks.

According to 2016 figures, the cyber protection market is valued at around US$4 billion of premiums written — with 90% written in the US and only 4% in Asia and other markets.

Post-pandemic, demand should increase, Chaudhry told IAN. But "whether existing pricing means the segment is an attractive line at present is not yet clear," he added.

Chaudhry said in the short-term, specialist cyber insurers are adopting an increasingly conservative approach with concerns of a potential spike in losses. There has also been a sizeable rise in claims notifications — particularly from ransomware and crime events.

In the medium to long-term, the cyber protection segment in Asia will "develop significantly," according to Chaudhry.

Marsh has predicted robust cyber growth for Asia. Quoting Munich Re and AIG data respectively, the broker in 2017 estimated US$1.5 billion of cyber premiums for the region by 2020; and that cyber uptake would grow from 9% to 40% in Singapore alone by this year.

While Marsh doesn't yet have updated figures, it's clear there is a growing demand in Asia.

Building cyber resilience for businesses will take a joint effort by regulators, cooperative (re)insurers and businesses awareness of cyber vulnerabilities.

As Chelly concluded: "With accelerated digital transformation, the challenge for companies within the current hard economic situation is ensuring the security of this transformation. This [includes] understanding required measures, the risk profile shift and financial support to proceed [smoothly] — therefore, it's critical to raise awareness across all industries and ensure a top-down approach with the government's support."

The next six to 12 months will be key.

MORE FROM: IN FOCUS