RISK

From threats to impact: Evolving cyber risk concerns in Asia

Not only has Asia become the global economic growth engine, it is also fast becoming a centre of innovation and home to much technological advancement, says **Marsh Asia**'s **Naureen Rasul**. These remarkable developments have heightened the existing cyber risks and created new vulnerabilities. In 2018, there were several major cyber attacks in the region.

In the latest World Economic Forum Executive Opinion Survey 2018, respondents were asked to identify and rank risks that they viewed as the most important for doing business in their respective markets in the next 10 years. Unsurprisingly, most placed cyber risks in the top five risk concerns (Exhibit 1).

China: With widespread adoption of digital payments and transaction technologies, China is one of the most digitally-connected and innovative countries in the world – a trend that has increased cyber attacks in recent years.

Hong Kong: One of the most-at-risk economies in Asia in terms of cyber security issues. In the past year, there were cyber attacks against one of the world's largest airlines, travel agencies, as well as its own health department.

India: The growing dependency on data and digitisation efforts has increased the risks of cyber attacks, threatening its economy and infrastructure. It is estimated that over 50% of the reported cyber attacks caused upwards of $500,000 in financial damages from lost revenue, customers and opportunities, as well as out-of-pocket expenses.

Indonesia: In terms of cyber resilience, Indonesia trails behind its regional peers. Businesses are susceptible to data fraud and theft due to the lack of security technologies and user awareness. To combat this, Indonesia has issued new regulations to provide some protection for personal data in electronic systems.

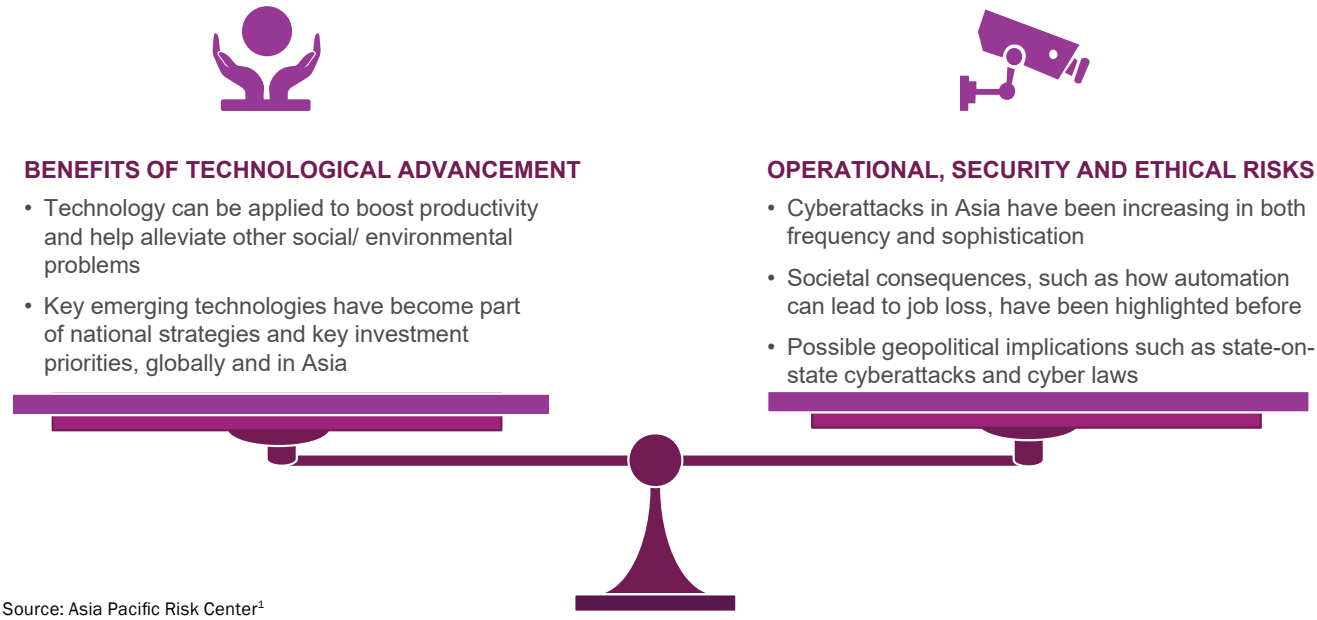
Japan: While Japan enjoys a

Exhibit 1: 2018 top risk concerns for doing business in the next 10 years for selected markets in Asia

Note: WEF Executive Opinion Survey (~12,500 responses worldwide). Results are based on about 2,500 responses across the region. Respondents could choose up to five risks which they viewed as being most important for doing business in their country. Top regional risks are calculated as the average across all countries of the proportion of respondents in each country identifying each risk as one of their five choices.

Source: World Economic Forum, Global Risks Report 2018, MMC analysis

Exhibit 2: Balancing benefits arising from rapid technological advancements



Source: Asia Pacific Risk Center[1]

relatively low crime rate, cyber attacks are on the rise – hacks against its cryptocurrency exchanges were up three-fold in 2018. These large-scale hacks not only highlighted the gaps in legislation for emerging technologies, but also exposed fault lines in its implemented cyber security measures.

Malaysia: Data fraud and theft and cyber attacks have increased in scale and severity, suggesting that businesses still lack a robust cyber security framework for detecting and countering cyber breaches. In early 2018, its central bank was attacked for a second time.

Singapore: Considered a world leader for its commitment to cyber security, cyber attacks continue to grow in frequency and impact. In July 2018, its largest group of healthcare institutions was hacked and the personal data of more than 1.5m patients was exposed.

South Korea: Government agencies, businesses and critical infrastructure have been the victims of several large scale cyberattacks. The latest hack took place in June 2018 when an estimated $30m worth of cryptocurrency was stolen from one of the major cryptocurrency exchanges.

Taiwan: Taiwanese companies are four times more likely to be susceptible to advanced cyber attacks than the global average. This has raised concerns around its lack of protection and complacency levels toward cyber security in recent years.

Thailand: Thailand is highly susceptible to cyber attacks. In August 2018, two banks were targeted by cyber attackers who stole non-financial data of about 123,000 customers. Low levels of encryption capabilities among businesses mean that they are especially prone to encryption-related cyber breaches.

Vietnam: In response to the surge in cyber attacks, the government has recently approved a cyber security law which mandates that global technology firms store important users' personal data and open offices locally.

Advances in technology have become the focus of many governments in Asia and features heavily in national development strategies. However, they are evolving faster than society's ability effectively to regulate and manage them. Governments must actively weigh the benefits of technology and prepare for the unknown operational, security and ethical problems arising from it – all can lead to the development of tighter cyber security frameworks, the enactment of tougher cyber security laws, as well as the creation of enhanced cyber insurance solutions.

In Asia, cyber insurance is becoming an integral part of a risk transfer strategy. The following losses stemming from a cyber breach can be insurable:

- Loss of income and increased costs of working resulting from network interruption caused by security failure, system failure, operational error, or failure of third party outsourced partners;
- Crisis response costs – IT forensic costs, legal expenses, customer call centre costs, notification expenses, identity theft remediation services and public relations costs;
- Costs of recovering, reconstructing, reloading, replacing digital assets which have been impaired due to a security failure, system failure, operational error, or failure of third party outsourced partners;
- Payment of cyber extortion losses and expenses; and
- Liability to third parties, defence costs and regulatory fines.

Ms Naureen Rasul is regional cyber practice leader with Marsh Asia

[1] MMC Asia Pacific Risk Center, 2018. From Threats to Impacts: Evolving Risk Concerns in Asia-Pacific Vol. 3