Myriad issues with SC's cyber risk guidelines

While observers say it is timely though late, cost of implementation, directors' unpreparedness and defining cyber risks are factors

by Ho Chung Teng

THE Securities Commission's *Guidelines on Management of Cyber Risk* which came into effect on Oct 31, will enhance the security of IT systems and benefit companies that outsource their cybersecurity services.

Among those expected to gain from the guidelines include Dataprep Holdings Bhd, Mesiniaga Bhd, Genetec Technology Bhd, Managepay Systems Bhd, Privasia Technology Bhd, Scan Associates Bhd and Systech Bhd.

Fund managers and analysts expect the guidelines to trigger short-term activity in those counters.

The SC's move to deal with cybersecurity risks by defining the role and responsibilities of corporate boards of directors and top management is viewed as a good move.

A fund manager says investors will ride on the guidelines. And he draws a parallel with the implementation of the Goods and Services Tax (GST) in April last year.

"There's currently nothing to move the stock market. Hence, the guidelines will serve as a catalyst for short-term investors. It is likely to taper off by the first half of next year.

"Most of the IT stocks' price-to-earnings ratio is high. Coupled with the poor market sentiment, I don't think it will sustain for long," says the fund manager.

JF Apex Securities Bhd head of research Lee Chung Cheng tells ***FocusM*** that the industry is still unsure about the mechanism and enhancements required of companies due to the guidelines.

He is also unsure if IT companies such as N2N Connect Bhd and Omesti Bhd will benefit substantially.

IT companies that gained from the GST hype last year included IFCA MSC Bhd and MyEG Services Bhd.

Their counters saw share prices and earnings boosted as a result of the expected demand for GST-related software.

IFCA saw its share price rally to an all-time high of RM1.67 in May last year, from an average of 10 sen per share in the first half of 2014.

For FY14 ended Dec 31, IFCA's net profit rose 12 times to RM20.76 mil from RM1.72 mil in 2013. For FY15, it reported a net profit of RM21.6 mil.

MyEG's net profit is also trending upwards. For FY16 ended June 30, its net profit rose to RM142.87 mil from RM24.84 mil in 2013.

The company's share price which was 67 sen in January 2014, closed at RM2.23 on Dec 7.

Heng says without the guidelines, market participants will not even look at cybersecurity as a concern

Timely move by SC

KPMG Management & Risk Consulting Sdn Bhd executive director Dani Michaux tells ***FocusM*** that the guidelines are timely.

She says market trends change quickly due to improved technology, and that cybersecurity breaches over the last six months have tripled compared to three years ago.

However, an IT security expert believes the guidelines' introduction is somewhat behind time.

He says cybersecurity has been a threat since the advent of computers, and that a number of major cyber attacks took place years ago.

Nonetheless, he reckons that the guidelines will result in better corporate governance. "At least the regulators are now forcing the board of directors to oversee their company's cyber risk," he says.

JONATHAN LOI/FocusM

Michaux says cybersecurity breaches over the last six months have tripled compared to three years ago

Tan says many many entities with in-house IT capabilities find it difficult to keep up with emerging technologies and cyber threats

Baker Tilly Monteiro Heng partner Andrew Heng concurs.

"Without the guidelines, I think market participants will not even look at cybersecurity as a concern, so I think it's timely that the SC has finally looked into it," he says.

Malaysian Alliance of Corporate Directors president Paul Chan says in the past two decades, the nature and composition of corporate asset values have significantly shifted from the physical to the virtual.

He cites Ocean Tomo's recent study *Intangible Asset Market Value*, which found that 80% of the total asset value of the Fortune 500 now consists of intellectual property (IP) and other intangibles.

US-based Ocean Tomo provides financial services related to intellectual property and intangible assets, including financial expert testimony, valuation, strategy consulting, investment advisory, innovation management consulting and transaction brokerage.

"Along with the rapidly expanding digitisation of corporate assets, there has been a corresponding digitisation of corporate risks.

"Consequently, policymakers, regulators, shareholders, and the public have become more attuned to corporate cybersecurity risks than ever before.

"Organisations are at risk of IP loss, declining public confidence, reputational risks, new legal and regulatory sanctions, and compromised, lost or altered data," Chan says.

He says such risks can adversely affect competitive positioning, stock prices, and shareholder values.

Effective governance

An SC spokesperson tells ***FocusM*** that it introduced the guidelines to enhance the cyber resilience of the capital market by requiring regulated entities to establish and implement effective governance and risk management measures.

"It helps inculcate a corporate culture of vigilant management of cyber risks, which is critical for a rapidly-evolving online environment as it minimises disruption to capital markets, ensures investor protection and preserves market confidence," he says.

The regulator says a dedicated cyber unit has been established to track and monitor emerging threats and occurances of cyber risks.

"As the reporting of cyber risk events is likely to be voluminous and wide-ranging, the SC will undertake a risk-based approach. We will put greater focus on more significant cyber breaches to ensure optimised allocation of resources," he says.

The spokesperson says transition arrangements are provided to allow the necessary preparation for compliance with the guidelines.

"During the transition period, the SC will continue to assess the issues and challenges faced by capital market intermediaries in managing cyber risks.

"While there are sanctions for non-compliance with the guidelines, what is imposed depends on the seriousness of

Companies not adequately prepared for cyber attacks

PWC Malaysia's risk assurance services' senior executive Tan Cheng Yeong says many entities with in-house IT capabilities find it difficult to keep up with emerging technologies and cyber threats.

"There is a growing trend of internal audit functions having outsourcing or co-sourcing arrangements with cybersecurity specialists.

"This serves to tap their expertise to address concerns raised by audit committees and the board of directors," he says.

Baker Tilly Monteiro Heng partner Andrew Heng says most companies are not ready to tackle cyber risks as they seem to rely on off-the-market products, such as antiviruses.

He says most board members are made up of the "older generation", who may not be familiar with the IT concept.

"You have to understand that these people grew up without much technology," he says.

Findings of a KPMG survey reveals that chief executives globally, including those in the country, continue to face challenges in terms of risks associated with cyber breaches and being fully prepared for a future cyber event.

"CEOs recognise there is work to be done to protect their organisations. Some 72% of them are not fully prepared for a cyber event," the report says.

While the Securities Commission's (SC) introduction of the Guidelines on Management of Cyber Risk, which came into effect on Oct 31, promotes good governance, it can also be expensive as companies incur higher compliance costs to enhance cybersecurity.

PwC's Tan says: "Most of the companies surveyed are not adequately prepared or even fully understand the risks they face. Only 35% of surveyed organisations have a cyber incident response plan."

He says its recent PwC Global Economic Crime Survey 2016 (Malaysia report) highlights that cybercrime is now the second most reported economic crime, and affects 30% of organisations.

the breach," he says.

Baker Tilly's Heng says for a start, a review of a company's IT system will cost between RM50,000 and RM100,000.

Once the review is done, a company could probably look at spending between RM200,000 and RM1 mil on cybersecurity, depending on its value chain, importance within the industry, and how much data the company has.

He says most companies are not spending substantial amounts on IT security at the moment.

"I think they need to budget a good sum of money for this, and not just for the IT infrastructure," he says.

KPMG's Michaux says the cybersecurity spend depends on how much a company wants to protect itself.

Citing global statistics, she says such spending tripled, and that companies spend 3%-4% of their IT budget on security. However, that number has recently increased to 9%-11%.

PwC Malaysia's risk assurance services senior executive Tan Cheng Yeong advises companies to conduct regular vulnerability assessments so that they can implement immediate "stop-gap" measures before perpetrators exploit vulnerabilities.

"In the medium-term, invest in security and event monitoring systems apart from an effective incident response system," Tan says.

In regards to high-risk companies, Tan says they need to invest in fundamental safeguards, including regular patching of firewalls, updating their firmware, upgrading systems with security and password settings, and securing devices.

High-risk sectors

While cyber risk affects almost everyone, Tan says capital market entities that are actively exploring new digital business channels are more susceptible to it.

"Smaller standalone entities which have fewer resources and operate at a more pragmatic level may need to implement greater changes," he says.

Heng says based on last year's records, the healthcare, manufacturing, financial services, government and transportation industries are among those susceptible to cyber risks.

"I think these are the current targets for hackers. But once the bigger companies improve their security, they [hackers] might look at the smaller companies, so it trickles down," he says.

Michaux says the biggest challenge for large organisations is to define cyber risk.

"The reason hackers breach a company is predominantly for information or to make money," she says.

She says there are four categories of cyber risk. The first involves activities or a hacktivist, next is organised crime, third insiders, and fourth nationally-sponsored cyber attacks.

"Victims of the last one are usually critical national infrastructure companies, organisations, oil related companies, power and telecommunications, because you can control the entire nation," she says.

Nevertheless, Michaux says with the onset of computers, every company has a certain element of cyber risk. FocusM