Publication: The Business Times Online
Date: 13 September 2017
Headline: Break down silos to manage your cyber risks

Break down silos to manage your cyber risks

If companies are to have a successful cybersecurity strategy that stands a higher chance of success, the whole of the business needs to break down the silos and come together, according to cybersecurity experts.

Cybercrime has become more pronounced in recent years as companies and economies become more interconnected and integrated.

“The borderless nature of the cyber economy also present opportunities for cyber criminals,” said John Lee, President of ISACA Singapore Chapter, which represents information systems governance professionals.

Increasingly, cybercrime is being viewed as a major business risk because of the impact that a cyber-attack could have on company operations, financial statements, legal exposure and brand reputation.

“Cybersecurity is essentially a business issue and not merely a technology issue - it should be addressed as part of corporate governance,” said Dr Calvin Chan, Director, Office of Graduate Studies at Singapore University of Social Sciences, who has consulted and published extensively on cybersecurity issues.
SEE ALSO: Future-proof your finance capability amid digital disruption

Dr Chan said while the actual execution of a cybersecurity strategy may be the responsibility of the Chief Executive Officer (CEO), the Chief Information Officer (CIO) or even the Chief Information Security Officer (CISO), these executives have to be accountable to the Board to ensure good corporate governance.

A lot of has changed very quickly in the cybersecurity realm in recent years.

Where previously it was largely a support function, today cybersecurity is front and centre for any organisation that relies on technology.

“Increasingly, it is the very fabric of the digital business itself,” said Mr Gerry Chng, partner and cybersecurity leader at professional services firm EY.

“As a result, you need to have the whole business come together and it is really the board and the management that need to be overall responsible and accountable for cybersecurity and bring the right resources into it,” Mr Chng added.

Experts say while it is tempting to assume that cybersecurity is a big organisation issue that does not affect smaller companies as significantly, this would be the wrong mindset.

“It can be a dangerous mentality as criminals are opportunists. As long as companies use or are connected to the Internet, they are potential targets,” said Mr Lee.

“The size of the business may not be a good gauge - a better gauge may be in terms of the extent of reliance on IT and the extent of cybersecurity risk exposure,” said Dr Chan.

For example, a big food and beverage chain that uses little technology may be less exposed to cybersecurity risk than a small technology start-up that creates mobile apps.

“From a hacker’s perspective, all they need to do is to target small companies that have business dealings with larger organisations to eventually gain a foothold into those organisations,” said Mr Chng.

To align a cybersecurity approach to organisational strategy, experts recommend that organisations look at cybersecurity risk assessment as another dimension of risk assessment, especially for strategy and projects that depend heavily on technology.

Publication: The Business Times Online
Date: 13 September 2017
Headline: Break down silos to manage your cyber risks

“The aim is not so much to eliminate cybersecurity risk, which is impossible to achieve. Instead, the aim is about managing cybersecurity risk by bringing it to an acceptable level for the company,” said Dr Chan.

But organisations also need to invest to build and sustain a robust cybersecurity strategy.

“An organisation's IT system and environment change with time, hence the (cybersecurity) process must adapt to the new environment and the new threat landscape,” said Prof Robert Deng, Dean, Postgraduate Research Programmes and AXA Chair Professor of Cybersecurity, Singapore Management University.

“You need to focus on how to effectively protect your IT systems and how to respond and recover in the event of an attack,” he added.

But a holistic strategy and a focus on the big picture are also key.

“Instead of worrying about what is the next type of cybersecurity threat and putting in-place counter measures reactively in a piece-meal manner, the wiser thing to do is to develop a systematic multi-layered cybersecurity strategy comprising measures for prevention, protection, detection, mitigation, respond and recovery,” said Dr Chan.

“This will avoid any single point of failure. Even in the unfortunate event of a cybersecurity incident, such a multi-layered strategy can also help to minimise the extent of damage,” he added.

Some observers say a good cybersecurity strategy is not about putting on more controls.

“It’s really about building this whole concept of digital trust,” said Mr Chng.

“Two other pieces that need to be in there are ‘sensing capabilities’ or knowing what’s going to happen - and that’s where analytics and data visualisation will come in,” he said.

Experts say companies will find it beneficial to take a risk-based approach to managing cyber threats.

“What’s most important to your business? And if you look at it from the hacker’s perspective, what is it that you have that would be of interest to them? How would they lay hands on the information that’s important to you and how do you then monitor whether those bad things are happening?” said Mr Chng.

It is also critical to address the most vulnerable element of the cyber protection chain.

“Staff can be one of the weakest links if they do not comply with policy and engage in unsafe cyber practices such as downloading files from untrusted websites, opening phishing emails, sharing passwords and connecting unsecured devices to the corporate computer,” said ISACA’s Mr Lee.

“The competence of the technical staff is important,” he added.

This series is brought to you by CPA Australia to share knowledge on topical issues relevant to business, finance and accounting.

Cyber resilience – step by step

- Regularly update your cybersecurity policies to follow the best practices in the industry
- Timely update and patch your IT systems and applications
- Deploy unified cybersecurity solutions that provide full visibility of the system and can detect and prevent attacks in their early stages
- Regularly backup your data so that data can be restored when needed

- Invest in better and more targeted user/employee cybersecurity training

Source: Singapore Management University

Every CEO should know if their organisation has cybersecurity under control

This is not about developing deep technical knowledge. It is about understanding how an organisation's cybersecurity approach relates to organisational and strategic priorities and protects the data that is vital to business success.

These four questions could be the start of a critical discussion with your Chief Information Security Officer (CISO) about the safety of your organisation:

1. Do you understand our wider business strategy?
2. Have you aligned our cybersecurity approach to our organisational strategy?
3. What are the gaps?
4. How are you evolving our cybersecurity approach to match the changing risk landscape?