INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS

60 Cecil Street ISCA House
Singapore 049709
TEL +65 6749 8060
FAX +65 6749 8061

Global Mindset, Asian Insights

18 August 2017

(By email: csa_cs_bill_feedback@csa.gov.sg)

To whom it may concern,

Public Consultation for the Cybersecurity Bill

The Institute of Singapore Chartered Accountants (ISCA) would like to thank Ministry of Communications and Information (MCI) and the Cyber Security Agency of Singapore (CSA) for the opportunity to provide feedback on the proposed Cybersecurity Bill.

ISCA is the national accountancy body of Singapore. ISCA's vision is to be a globally recognised professional accountancy body, bringing value to our members, the profession and wider community. There are over 32,000 ISCA members making their stride in businesses across industries in Singapore and around the world.

Now more than ever, companies need a strong cyber-risk management framework in place to deal with increasing cybersecurity threats.

Our key comments/recommendations are as appended below.

1) Important role of cybersecurity service providers (CSPs)

We are cognisant of the government's intention to strike a balance between light-touch regulation and a regime that sufficiently protects CIIs at the national level. In reality, many organisations rely on CSPs for assessing and implementing appropriate security measures due to costs, lack of sufficient in-house expertise, etc. As such, CSPs must be held to a high level of accountability.

Under the Bill, CII owners will be subjected to criminal penalties under Section 10. However, there are no such equivalent measures on CSPs, who play an important role in instituting the appropriate security measures and whose full cooperation is needed in a cybersecurity incident. Furthermore, we noted that CSPs are currently not accredited or licensed by the authorities, though there are plans to do so over time. Hence, given the above considerations, the current Bill appears to place undue burden on CII owners.

We recommend the Bill to consider making both the CSPs and CII owners have shared responsibility in ensuring cybersecurity of the CIIs.

INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS

60 Cecil Street ISCA House
Singapore 049709
TEL +65 6749 8060
FAX +65 6749 8061

2) Greater clarity on third and fourth party liability

The cybersecurity framework of CII owner may involve outsourcing of certain tasks and aspects to a number of service providers. For instance, the cybersecurity service and software is outsourced to a vendor, who may themselves outsource some aspects of their own services and products to yet another service provider. The Bill should provide greater clarity on the issue of liability and responsibility in the event of a cybersecurity incident, with regard to third and fourth parties.

Imagine a scenario in which a CII owner hosts a databank on a cloud-based system, which is then hit by a cybersecurity incident. How is liability and responsibility to be fairly apportioned between the CII owner and the cloud service provider, and possibly yet other third-party service providers? As cited above, the full co-operation of the CII owner and all service providers involved is needed for timely rectification of a cybersecurity incident.

3) Compliance audits and auditors

Section 16 of the Bill requires CII owners to conduct a compliance audit at least once every three years, with respect to the Act, codes of practice and standards of performance, to be carried out by an auditor approved or appointed by the Commissioner.

The Bill should provide more clarity on what constitutes an auditor in this context such as the competencies required, and what professional standards they are to be subjected to. This would provide more consistency in the standard of the audit. A skills framework for auditors in this space would be welcomed.

We recommend that the Bill consider tailoring the frequency of audits for the 11 critical sectors according to the nature of the industry. For example, the Bill may consider requiring more frequent audits for industries with businesses handling highly sensitive data and/or are frequently targeted for cyberattacks.

We are cognisant of the additional resources that organisations need to expend as a result of more frequent audits. However, given CII owners are subjected to criminal penalties in the event of failure to execute their duties under Section 10, CII owners are unlikely to be averse to and may in fact appreciate more frequent audits, during which the CSA could be given the opportunity to articulate any concerns on the CII more precisely and in a timely manner.

INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS

60 Cecil Street ISCA House
Singapore 049709
TEL +65 6749 8060
FAX +65 6749 8061

4) Clarity and guidance on the term "significant" cybersecurity incident

CII owners would appreciate greater clarity and guidance on what constitutes a "significant" cybersecurity incident.

5) Clarification on ethics & requirements in the regulation of cyber security service providers

The Bill should clarify what code of ethics or list of requirements cybersecurity service providers should adhere to, or if perhaps a new code of ethics or lists of requirements is to be drafted by an appropriate body. For example, members of ISCA must adhere to Ethics Pronouncement (EP) 100 Code of Professional Conduct and Ethics issued by ISCA (ISCA Code).

Additionally, it should be noted that it is a challenge to define what constitutes "assurance on security and safety", which cybersecurity service providers are to render to CII owners, given the absence of any such code or list of requirements.

6) Cybersecurity training is key

Key to achieving compliance with the Bill's provisions on cybersecurity is training, besides the use of penalties. The legislation of the Bill would likely lead to CII owners having to expend resources to invest in compliance, which is a cost to business. To get CII owners up to speed on compliance on cybersecurity, as well as to incentivise organisations to build a cyber-aware culture, the government may (as a catalyst) wish to consider providing a subsidy towards training courses on cybersecurity. This would also encourage non-CII sectors to undergo training and implement cybersecurity measures, which further strengthens Singapore's cybersecurity strategy.

As work is increasingly digitalised, all professions need to have awareness on cybersecurity. In this regard, ISCA recognises the importance of cybersecurity and continues to roll out numerous cybersecurity training courses. Such courses can help organisations' employees in developing cybersecurity awareness which would go towards building a cybersecurity strategy for their business, developing policies and procedures for the development of a cyber security risk management process etc. Thus, trade associations and chambers (TACs) are important touch points underpinning cybersecurity preparedness in the economy and are well placed to offer such training to their members. The government can consider how to leverage the TACs as part of its national cybersecurity strategy.

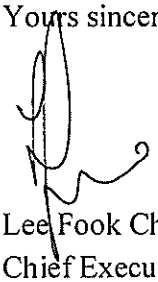
INSTITUTE OF
SINGAPORE
CHARTERED
ACCOUNTANTS

60 Cecil Street ISCA House
Singapore 049709
TEL +65 6749 8060
FAX +65 6749 8061

Global Mindset, Asian Insights

I thank you for providing ISCA, the national accountancy body, with the opportunity to provide feedback on the Cybersecurity Bill. I hope you and your team will find the feedback useful.

Yours sincerely,



Lee Fook Chiew
Chief Executive Officer
Institute of Singapore Chartered Accountants