Submission of consolidated comments on behalf of the NTU Cyber Risk Management (CyRiM) project to the Personal Data Protection Commission Singapore: "Public consultation for approaches to managing personal data in the digital economy"

Background:

Young and research-intensive, Nanyang Technological University (NTU Singapore) is ranked 11th globally (QS World University Ranking 2018). It is also the world's top young university.

Nanyang Business School at NTU leads a government-industry-academia research endeavour – the NTU Cyber Risk Management project (CyRiM)). This is supported by the Monetary Authority of Singapore, the Singapore Cyber Security Agency, leading global insurance companies and the Geneva Association comprising 80 CEOs of the largest global insurance groups. Five global insurance companies (Aon, Lloyd's, MSIG, SCOR, and TransRe) provide financial support.

The CyRiM project is developing a theoretical framework for economic analysis that should 1) enable the optimisation of cybersecurity investment by firms and customised insurance policy; and 2) provide independent public policy recommendations to enhance cyber resilience. The project aims to support Singapore ambitions to become an industry centre of excellence on cyber risk.

The comments below reflect the perspective on this public consultation from several experts on the CyRiM project governing board with experience across the fields of insurance and risk management.

Contact person: Caitríona Heinl, Research Fellow, NBS, NTU Singapore (email: cheinl@ntu.edu.sg)

CyRiM comments part 1

5 Need for Mandatory Data Breach Notification

5.1 With Singapore's Smart Nation initiative and push towards a Digital Economy, personal data will increasingly be capitalised to deliver more innovative services and improve lives. This, however, brings with it heightened risks and impact of data breaches for individuals. Gemalto, a digital security organisation, reported that compared to 2015, 2016 saw a 86% increase in data records lost or stolen worldwide. Identity theft was the leading type of data breach since Gemalto started tracking breach incidents in 2013.

5.2 To strengthen protection for individuals and build confidence in organisations' management and protection of personal data, PDPC is proposing to introduce a mandatory data breach notification regime under the PDPA.

5.3 With mandatory data breach notification, affected individuals who are notified of the data breach will have the opportunity to take steps to protect themselves from the risks or impact from the data breach while affected organisations will be able to receive guidance from PDPC on post-breach remedial actions when they notify PDPC. Overall, this will enable PDPC to better oversee the level of incidences and management of data breaches at the national level.

CyRiM Comments

5.4 Mandatory Data Breach Notification will enhance disclosure requirements, and promote greater transparency in the way public and private sectors respond to data breaches. In turn, this will also give firms and individuals greater impetus to practice better cyber hygiene, as well as to take steps to be aware of, measure and mitigate their cyber risks (eg. via having an incident response plan, insurance protection).

5.5 The role of cyber insurance, as part of a holistic cyber risk mitigation strategy, is an important one. Cyber insurance is closely linked with building overall cyber resilience, as it facilitates:

5.5.1 **Pricing and Managing Cyber Risks-** It helps to put a price on firms' cyber risk through the premiums that they pay, and through this pricing mechanism creates incentives for firms to mitigate cyber risk. It also spurs preventative action as firms benefit from the insight of their insurers on claims and near misses, which in the case of cyber risk is particularly valuable due to the lack of sufficient information of this emerging risk where losses often go unreported.

5.5.2 **Responding to Cyber Breaches -** Cyber Insurance helps ensure a speedy, coordinated and comprehensive response to cyber breaches which is important in reducing the cost of cyber breaches. The Ponemon Institute's 2017 report estimates that cyber insurance brings down the per capita cost of data breach by US$5.40 whilst incident response (which Cyber Insurance helps partly pay for) brings down this cost by US$19.30. Whilst cyber coverage varies from policy to policy, a typical cyber insurance policy should be able to cover response costs of:

- Investigation- eg. costs of a forensics investigation to determine what happened, its repair and how to prevent it. This may involve the services of a third party security firm as well as coordination with CSA, and other agencies.
- Business losses- this could include monetary losses from data destruction, network downtime, business interruption, denial of service and costs involved in managing a crisis, including reputation damage.
- Notification- this includes notification to customers and other affected third parties as well as credit monitoring for parties whose information was or may have been breached.

As a result, demand for cyber insurance tended to grow in tandem with the development of mandatory data breach notification laws. The US, where 47 of the 50 states have mandatory data breach notification laws, accounts for 90% of global cyber insurance premiums. With EU's upcoming Global Data Protection Regulation (GDPR) mandating cyber breach notification in effect in 2018, which will also apply to the UK, there has been an uptick in cyber insurance purchase in the UK and EU. This has also been the case in Australia, which mandated data breach notification in February this year. This is because cyber insurance policies, in addition to covering business downtime and IT damage costs, typically also cover costs stemming from mandatory data breach notification, including notification of authorities and affected parties, forensics and IT investigation costs, regulatory fines and PR related costs to manage reputation.

CyRiM Comments part 2

	PDPC proposals - Singapore	**Comments**
Data breach notification	According to para 6.13 of the consultation, where a data breach meets the criteria for notifying PDPC under the PDPA, PDPC proposes to require that the organisation notifies the PDPC as soon as practicable, no later than 72 hours from the time it is aware of the data breach.	This is in line with the requirements under the GDPR.
Communication of a personal data breach to the data subject	Para 6.2 of the consultation: "Organisations must notify affected individuals and PDPC of a data breach that poses any risk of impact or	Suggest rewording the sentence to read as follows: Organisations must notify affected

	harm to the affected individuals”	individuals and PDPC of a data breach that poses a high risk of impact to the rights and freedom of natural persons or harm to the affected individuals”
Significant scale of breach	Para 6.2: “organisations must notify PDPC where the scale of the data breach is significant, even if the breach does not pose any risk of impact or harm to the affected individuals. PDPC is proposing for a data breach involving 500 or more affected individuals to be considered a significant scale that would need to be notified to the regulator.	Propose that instead of prescribing a specific number, PDPC provide guidance on the types of factors to take in to account when considering what is significant (e.g. Data types, number of individuals, likely impact etc).