Managing Data Breaches: The PDPA Perspective

by Thong Xin Lin

In the past year or so, it has become apparent that organisations, big and small, have been vulnerable to security breaches as a result of hacking or data theft.

Facebook, one of the world's largest social networking platforms, is embroiled with the recent Cambridge Analytica scandal which allegedly harvested up to 87 million Facebook user accounts without proper disclosure or permission.[1] Mobile phone subscribers in Malaysia suffered a similar fate when the personal details of approximately 46.2 million subscribers were exposed online for a period of time.[2]

Security breaches can have far-reaching consequences, with organisations typically facing operational disruptions, reputational loss, and hefty fines. In the age of technology and innovation, information and data are vital to business operations, and therefore, business organisations have an interest to manage its operations in a responsible manner and ensure the security of the information and data that they possess.

Security obligations

In Malaysia, the use of personal data in commercial transactions is regulated by the Personal Data Protection Act 2010 (PDPA),[3] which has been in force since 15 November 2013. In particular, organisations that use personal data in the course of their business operations are required to take steps to protect it from any unauthorised access, disclosure or loss. A data leak may potentially expose the organisation to prosecution for failure to take practical steps to protect the personal data.[4]

Other countries impose similar obligations relating to data security under their personal data protection laws.[5]

Data breaches

Managing a data breach from the point of its first discovery will enable the incident to be handled in an orderly and precise manner, whereby steps to mitigate any consequences of the breach can be executed as early and as effectively and efficiently as possible.

The Personal Data Protection Commissioner has power to issue standards in relation to security, retention and data integrity.[6] In the past, the Commissioner has issued the Personal Data Protection Standards 2015 to set out the minimum requirements in relation to security, retention and data integrity.[7] However, specific guidance on how data breach incidents should be handled have yet to be

1 David Ingram "Facebook says data leak hits 87 million users, widening privacy scandal" *Reuters* (5 April 2018) <https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM>

2 Royce Tan and Sharmila Nair, "M'sia sees biggest mobile data breach" *The Star Online* (31 October 2017) <https://www.thestar.com.my/news/nation/2017/10/31/msia-sees-biggest-mobile-data-breach-over-46-million-subscribed-numbers-at-risk-from-scam-attacks-an/> Separately, it was reported in January 2018 that the personal details of more than 200,000 Malaysian organ donors and their next of kin was leaked online: Sharmila Nair, "Another data breach — now it's organ donor info" *The Star Online* (24 January 2018) <https://www.thestar.com.my/news/nation/2018/01/24/another-data-breach-now-its-organ-donor-info/>

3 [*Act 709*]

4 The failure of a business organisation to protect the personal data within its control amounts to an offence under the PDPA, and if convicted, the organisation is liable to a fine not exceeding RM300,000 and/or imprisonment for a term not exceeding two years.

5 For example, Singapore (Personal Data Protection Act 2012, s 24), the UK (Data Protection Act 1998, para 7, Part 1, Schedule 1) and Hong Kong (Personal Data (Privacy) Ordinance, para 4, Schedule 1).

6 This is pursuant to Regulations 6, 7 and 8 of the Personal Data Protection Regulations 2013.

7 Non-compliance amounts to an offence and the data user will be liable to a fine not exceeding RM250,000 and/or imprisonment for a term not exceeding two years.

issued. On the other hand, financial service providers under the purview of the Central Bank of Malaysia are required[8] to have a response plan and notify[9] the relevant stakeholders in the event of a customer information breach.

Until some specific guidance becomes available, organisations in Malaysia can consider adopting models provided in other countries to mitigate the negative consequences of a data breach.[10] If an organisation were to adopt a response procedure, it should take into account the consideration below:

Containing the breach

An organisation should act as soon as it is aware of a data breach. In taking steps to contain the breach, it should consider the following (where applicable):

- Shut down the compromised system that led to the data breach;

- Establish whether steps can be taken to recover lost data and limit any damage caused by the breach; for example, remotely disabling a lost notebook containing the personal data of individuals;

- Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system and remove external connections to the system;

- Notify the relevant law enforcement agencies if criminal activity is suspected and preserve evidence for investigation, for example, hacking, theft or unauthorised system access by an employee.[11]

Assessing risk and impact

It is vital that risk and impact of the data breach is properly assessed to enable organisations to respond to public enquiries and to determine the next steps to be taken. The potential impact as a result of a data breach includes threat to personal safety, identity theft, financial loss, reputational damage, and loss of business and employment opportunities. Some considerations to be taken into account, to determine the extent of the impact depends on:

- The number of individuals affected: A large number may not mean a higher risk, but assessing this helps overall risk assessment;[12]

8 On 17 October 2017, the Central Bank of Malaysia issued the guidelines for "Management of Customer Information and Permitted Disclosures", which sets out the requirements for measures and controls in handling customer information throughout the information lifecycle in line with applicable laws. Non-compliance may result in enforcement action. Among others, financial service providers are required to:
(a) have in place a customer information breach handling and response plan;
(b) contain a customer information breach immediately;
(c) carry out an investigation to ascertain the root causes of a customer information breach which must generally be completed within three months upon detecting the breach;
(d) submit a detailed investigation report to the Central Bank of Malaysia within one working day upon tabling to the board; and
(e) record all customer information breaches.

9 Under the aforementioned guidelines for "Management of Customer Information and Permitted Disclosures", financial service providers must notify:
(a) the Central Bank of Malaysia immediately upon discovery of a breach where the breach is likely to pose reputational risk to financial service providers or a threat to public confidence and trust; and
(b) the relevant law enforcement agency if the breach appears to involve fraud, criminal activity or may result in identity theft.
A public announcement may need to be made to notify customers if the breach affects a substantial number of them.

10 In Australia, the Notifiable Data Breaches scheme which incorporates requirements for mandatory data breach reporting came into effect on 22 February 2018. The EU General Data Protection Regulation, which is expected to come into effect on 25 May 2018, will require organisations to notify the supervisory authority and the affected individuals where the incident is likely to result in a risk to the rights and freedoms of natural persons. Singapore is also in the midst of seeking public consultation on the review of its Personal Data Protection Act 2012, which includes matters relating to mandatory data breach notification.

11 This is a summary of guidance available in Singapore (see the "Guide to Managing Data Breaches" issued by the Personal Data Protection Commission Singapore on 8 May 2015) and Hong Kong (see the "Guidance on Data Breach Handling and the Giving of Breach Notifications" issued by the Office of the Privacy Commissioner for Personal Data, Hong Kong in October 2015).

12 Following responses from the public, the Personal Data Protection Commission Singapore has stated that it intends to retain the criterion of significant scale of breach for notification to Personal Data Protection Commission Singapore but will not prescribe a statutory threshold for number of affected individuals.

- The identity of the affected individuals: Different people will face varying levels of risk as a result of a loss of personal data. For example, the unauthorised disclosure of personal data belonging to former convicts will likely carry a higher risk than the personal data belonging to the employees of an organisation;

- The type of personal data involved: The more sensitive the data is, the greater the damage it may cause to the affected individuals;

- The steps that have been taken after the data breach; and

- The ability of the data subjects to avoid or mitigate possible harm.[13]

Reporting the incident

The data breach reporting mechanism is presently being made a feature in the data protection laws of many countries.[14] Data breaches are usually only required to be reported if it results in some form of harm to the affected individuals.[15]

The fact that Malaysia presently does not have any requirements on notifying data breach incidents will not allay public disgruntlement when affected individuals discover that an organisation has attempted to cover up the data breach, instead of notifying them about the incident. This was evident when the information of 46.2 million mobile number subscribers was exposed to the public and could not be accounted for by the MCMC[16] or the relevant third party service provider. A civil suit has reportedly been brought against these two parties for failing to guarantee the safety of the personal data of mobile users, which was apparently motivated by the inaction by the MCMC, including the lack of information on why and how the data breach happened, or the measures that have been taken to contain the breach.[17]

The inaction in the wake of a data breach exposes the affected individuals to harm, for example, if the stolen data is used for identity theft. In such a situation, any attempt to cover up the incident, as was attempted by Uber,[18] would seal the complicity of the organisation in the data breach, even if the organisation was a victim to the incident in the first place. Facebook and Cambridge Analytica now face a class-action lawsuit for allegedly misusing personal data. The complicity of Facebook lies with its failure to responsibly manage the breach when it was initially discovered several years ago.[19]

13 *Supra* n 11. Reference was also made to Australia's Privacy Amendment (Notifiable Data Breaches) Act 2017 and the UK's Privacy and Electronic Communications (EC Directive) Regulations 2003, to determine whether a reasonable person would conclude that a data breach would result in serious harm to any of the individuals.

14 In Australia, the Notifiable Data Breaches scheme which incorporates requirements for mandatory data breach reporting came into force on 22 February 2018. Other countries such as the EU (through the EU General Data Protection Regulation expected to come into force on 25 May 2018), Canada (which passed the Digital Privacy Act in June 2015), and Singapore (which has sought public consultation paper on the review of its Personal Data Protection Act 2012) have also taken steps to incorporate data breach notification mechanisms into their legislature.

15 Note that in most countries, the requirement to notify must be fulfilled where there is a concern that the data breach will result in some form of harm to the affected individuals. In Australia, the need to notify only arises if the data breach amounts to an "eligible data breach" under Australian data protection laws — this involves an objective assessment of whether the data breach is likely to result in serious harm to any of the individual to whom the information relates. Similarly, the EU General Data Protection Regulation will only require notification if there is a risk to the rights and freedoms of natural persons.

16 The Malaysian Communications and Multimedia Commission

17 Seri Nor Nadiah Koris, "MCMC, Nuemera sued over data breach in 2014" *New Straits Times* (7 February 2018) <https://www.nst.com.my/news/crime-courts/2018/02/333027/mcmc-nuemera-sued-over-data-breach-2014>

18 Governments around the globe launched investigations into Uber following the ride-hailing firm's admission that it had paid hackers US$100,000 (RM400,000) to cover up a breach that exposed the personal data of 57 million customers and drivers. For further information, see Jim Hinkle and Heather Somerville, "Regulators to press Uber after it admits covering up data breach" *Reuters* (22 November 2017) <https://www.reuters.com/article/us-uber-cyberattack/regulators-to-press-uber-after-it-admits-covering-up-data-breach-idUSKBN1DL2UQ>

19 Owen Bowcott and Alex Hern "Facebook and Cambridge Analytica face class action lawsuit" *The Guardian* (10 April 2018) <https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit>

While the idea of notifying the affected individuals and regulators of the data breach can be daunting, informing affected individuals of the breach allows individuals an opportunity to mitigate loss and damage ensuing from the incident. Where a civil lawsuit is brought, the claimant has to show proof of loss.[20] Informing affected individuals of the incident is in the interest of the organisation as it enables the affected individuals to take preventive measures against the incident, thereby minimising any potentially adverse impact that the incident has on them.

Thus, a response plan that encompasses a notification mechanism to relevant stakeholders is vital for organisations, even if it is not presently required under Malaysian law.

The legal element: Minimising liability

Reporting a breach does not ensure that an organisation escapes liability. However, if the breach is notified to the relevant stakeholders in a manner that is effective and efficient, the adverse impact of the breach can be minimised under the guidance of supervisory authorities.

Most regulators require a data breach to be notified within a prescribed time limit[21] and that affected individuals are also notified:[22]

- Notification to the supervisory authorities is made to allow the possibility for the supervisory authorities to advise the organisation on post-breach remedial actions;
- Notification to the affected individuals is made to enable the affected individuals to take their own precautionary steps to avoid any potential harm the data breach may result in.[23]

The human element: communicating the incident

There will be pressure from affected individuals for a detailed explanation of the data breach, while the organisation may be reluctant to reveal the full extent of the incident.

As a guide, organisations must provide sufficient information so that the affected individuals are able to understand the impact of the data breach, and where their identity and security may be compromised, these individuals can then take remedial measures. This information should include:

- Basic details of the data breach;
- Type of personal data involved;
- Steps that the organisation has taken or will take in response to the risks brought about by the data breach;
- Recommended steps to be taken by the individuals in response to the data breach; and
- Contact details of the officer managing the data breach.[24]

20 Additionally, the UK's Data Protection Act 1998 specifically recognises that an individual is entitled to compensation from the data user (i.e. the organisation processing the personal data) (referred to as "data controller" in the UK) if he suffers damage as a result of any contravention by the data user (see s 13(1)). This damage includes both material (i.e. monetary) and non-material (i.e. emotional) damage: *Vidal-Hall v Google, Inc* [2015] EWCA Civ 311.

21 The EU General Data Protection Regulation, expected to come into force in May 2018, would require data users to report a data breach to the supervisory authority within 72 hours after becoming aware of it (if it is likely that the data breach will result in a risk to the rights and freedoms of natural persons), whereas the notification to affected individuals is only required if the breach is likely to result in a high risk to the rights and freedoms of natural persons. It appears that this is the approach many countries are adopting: Australia requires the notification to be made first to the Australian Information Commissioner before notifying the affected individuals; Singapore has proposed for notification to the Singaporean Personal Data Protection Commissioner within 72 hours, while reporting to affected individuals is proposed to be done on a "as-soon-as-possible" basis.

22 For example, Australia has made this mandatory pursuant to the Privacy Amendment (Notifiable Data Breaches) Act 2017. In other countries such as the UK, Singapore and Hong Kong, it is recommended that the breach is reported to both the supervisory authorities and the affected individuals.

23 This is the general approach taken by supervisory authorities around the globe, including Australia, the UK, Singapore, Hong Kong and the EU, towards data breach notification.

24 *Supra* n 11

The notification of the data breach should be made directly to the affected individuals. In some circumstances, the organisation may be compelled to make a public announcement of the incident instead,[25] in which case additional consideration must be given to ensure that any information disclosed will not be used by unscrupulous parties.

Learning from the incident

After steps have been taken to contain and resolve the data breach, the organisation should examine the incident and its causes in order to make any necessary changes to existing systems and procedures in the future. Depending on the nature of the incident, the organisation should examine, for example, whether there are any inherent weaknesses in existing security measures such as the use of outdated software and protection measures, or whether employees have been sufficiently trained to handle data breach incidents.[26]

Organisations in Malaysia should be proactive in adopting global standards and anticipate the impending change that will inevitably reach our legislative shores. **LH-AG**

About the author

Thong Xin Lin (txl@lh-ag.com) is an associate with the TMT Practice, and is part of a team headed by Adlin Abdul Majid. She was one of two associates at Lee Hishammuddin Allen & Gledhill named by *The Legal 500 Asia Pacific 2018* to its 'Next Generation Lawyers' list for TMT.

Adlin Abdul Majid (aam@lh-ag.com) is a partner in the TMT Practice and also heads the Regulatory & Compliance team.

25 There are instances when a public notification can be made instead of notifying the affected individuals directly. This includes where the data subjects are not identifiable immediately or public interest exists (see the "Guidance on Data Breach Handling and the Giving of Breach Notifications" issued by the Office of the Privacy Commissioner for Personal Data, Hong Kong in October 2015). Additionally, where it involves disproportionate effort to notify the affected individuals directly, for example, where it is not practicable to notify each of the affected individuals of the data breach, a public notification can be considered (see the EU General Data Protection Regulation, Art 34(3)(c) and Privacy Amendment (Notifiable Data Breaches) Act 2017), s 26WL(2)(c)).

26 *Supra* n 11