DREW & NAPIER

Data Breach Notification: Requirements and Practices

12 May 2020

David N. Alfred
Director and Co-Head, Data Protection, Privacy & Cybersecurity Practice
Co-Head and Programme Director, Drew Data Protection & Cybersecurity Academy

AT A GLANCE

- Overview of Data Breaches in Singapore
- Data Breach Notification Requirements
- Data Breach Management

DATA PROTECTION ENFORCEMENT

Year	No. of Reported Decisions
2016	22
2017	19
2018	29
2019	52*

* Including cases without grounds of decision published

- Total number of reported decisions up to end-2019: **122**
- Contravention of the Protection Obligation is the most common (see earlier presentation)
- Total amount of financial penalties imposed up to end-2019: **S$2,036,000**
- *Highest financial penalty imposed on a single organisation: **S$750,000**
- *Highest cumulative financial penalties for a single data breach case: **S$1 million**

(*SingHealth case)

DREW & NAPIER

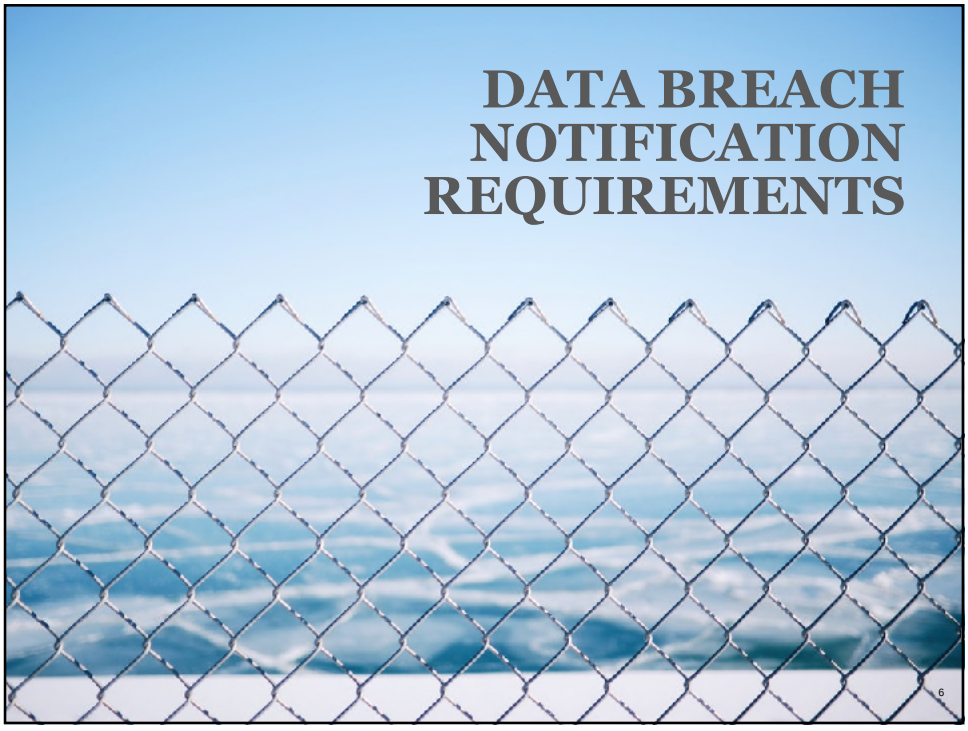
4

TYPES OF DATA BREACHES

- Deliberate disclosure of personal data
- Poor technical security arrangements
- Poor physical security arrangements
- Errors in mass email/post
- Insufficient data protection policies

DREW & NAPIER

5



6

OVERVIEW OF THE CURRENT REGULATORY REGIME

- Section 24 of the PDPA requires organisations to make reasonable security arrangements to protect personal data in their possession or under their control. In the event of a data breach or other security incident, there is presently no mandatory requirement to notify.
- **Notification to PDPC is purely voluntary.**
- Organisations are encouraged to notify.
- Should a notification of a data breach be made, the PDPC will decide if it will open an investigation into the data breach. Depending on the PDPC's findings, it may impose directions, including financial penalties, after it has concluded its investigation of the data breach.
- PDPC may take the notification into account as a mitigating factor.

CURRENT REGULATORY REGIME – WHO TO NOTIFY?

- Who to notify?

1) PDPC

2) Affected individuals

CURRENT REGULATORY REGIME – WHEN TO NOTIFY?

- Organisations are encouraged to notify the **PDPC** if a data breach is:

  a) likely to result in significant harm or impact to the individuals to whom the information relates;

  Or

  b) of a significant scale (i.e., data breach involves personal data of 500 or more individuals).

- Organisations are also encouraged to notify the **affected individuals** if the data breach falls into category a) above (i.e. is likely to result in significant harm or impact to the individuals to whom the information relates

CURRENT REGULATORY REGIME – HOW TO NOTIFY?

- **Notification to PDPC**: Notification should be submitted to the PDPC via its dedicated breach notification website (available at https://eservice.pdpc.gov.sg/case/db), and the following information should be included in the notification:
  - Extent of the data breach;
  - Type(s) and volume of personal data involved;
  - Cause or suspected cause of the breach;
  - Whether the breach has been rectified;
  - Measures and processes that the organisation had put in place at the time of the breach;
  - Information on whether affected individuals of the data breach were notified and if not, when the organisation intends to do so; and
  - Contact details of person(s) whom the PDPC could contact for further information or clarification.

CURRENT REGULATORY REGIME – HOW TO NOTIFY?

- **Notification to Individuals**: Notification to the affected individuals should contain the following:
  - How and when the data breach occurred;
  - Types of personal data involved in the data breach;
  - What the organisation has done or will be doing in response to the risks brought about by the data breach;
  - Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused;
  - Contact details and how affected individuals can reach the organisation for further information or assistance (e.g. helpline numbers, e-mail addresses or websites); and/or
  - Where applicable, what type of harm/impact the individual may suffer from the compromised data.

PROPOSED MANDATORY DATA BREACH NOTIFICATION FRAMEWORK

- According to the PDPC, the present voluntary approach has resulted in uneven notification practices across organisations – some will notify; others will not.
- In addition, with Singapore's Smart Nation initiative and a push towards a Digital Economy, personal data will be increasingly capitalised to deliver more innovative services and improve lives – but this brings with it heightened risks and impact of data breaches for individuals.
- In order to strengthen protection for individuals and build confidence in organisations' management and protection of personal data, PDPC will be introducing the Data Breach Notification Framework in the next review of the PDPA, which chiefly introduces the **mandatory breach notification obligation**.
- Public consultation exercise conducted from mid-2017 to early-2018 – 68 responses received from the public.

PROPOSED MANDATORY FRAMEWORK – CRITERIA FOR NOTIFICATION

- **Risk of impact or harm to affected individuals**: Organisations must notify affected individuals and PDPC of a data breach that poses any risk of impact or harm to the affected individuals.
  - PDPC has indicated that it would issue Advisory Guidelines to clarify what it means by "*any risk of impact of harm*", but has set out some examples of data breaches that pose "*any risk of impact or harm*" as those that involve personal data such as:
    - NRIC numbers
    - health information
    - financial information
    - Passwords
  - In response to public feedback, PDPC will be rephrasing this criterion to "*likely to result in significant harm or impact to the individuals to whom the information relates*".

PROPOSED MANDATORY FRAMEWORK – CRITERIA FOR NOTIFICATION

- **Significant scale of breach**: 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.
  - The initial approach is for "*significant scale*" to be set at 500 people, although this was met with disagreement from the public responses elicited.
  - PDPC has indicated, in its response to the public consultation, that it would be retaining the requirement for the breach to be on a "*significant scale*" but would not prescribe a statutory threshold for the number of affected individuals.

PROPOSED MANDATORY FRAMEWORK – TIME FRAME FOR NOTIFICATION

- **For notification to PDPC – as soon as practicable, and no later than 72 hours**: Organisations will have to notify the PDPC as soon as practicable, and in any even no later than 72 hours, from the time it is aware of the data breach.
  - The cap of 72 hours "*provides clarity for organisations as to the definitive time by which they would have to notify PDPC*"
  - This is similar to Article 33 of the GDPR, which states that "*In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority …*"
  - In response to public feedback that 72 hours was too short a period of time, PDPC indicated that it intends to provide for an assessment period of up to 30 days from the day the organisation first becomes aware of a suspected breach, to assess its eligibility for notification. This follows Australia's notifiable breach scheme.

PROPOSED MANDATORY FRAMEWORK – TIME FRAME FOR NOTIFICATION

- **For notification to individuals – as soon as practicable**: Organisations will be required to notify all affected individuals, if the breach meets the notification requirement, as soon as possible.
  - In view of the variability of data breach circumstances, PDPC will not be imposing a time cap for notification to individuals.
  - Organisations must notify the affected individuals as soon as practicable, from the time the organisation determines that the breach is eligible for reporting, regardless of whether it has fully utilised the 30-day assessment period.

PROPOSED MANDATORY FRAMEWORK – MODE OF NOTIFICATION

- **PDPC does not intend to prescribe the mode of notification to PDPC and affected individuals**: PDPC recognises that there are many different modes of notification that could evolve with technology, and that organisations should be allowed to determine the most efficient and expedient mode of notification to comply with the breach notification requirement to inform affected individuals as soon as practicable so that they may take actions to mitigate the potential risk of harm or loss from the breach.
  - PDPC will issue Advisory Guidelines to provide guidance for organisations on complying with the data breach notification requirements when introduced.

OTHER DATA BREACH NOTIFICATION REGIMES IN SINGAPORE

- The Cybersecurity Act 2018 (Act 9 of 2018) requires owners of Critical Information Infrastructures ("**CIIs**") to notify the Commissioner of Cybersecurity of data breaches involving CIIs.
- There are several sectorial regulators that impose their own data breach and/or cybersecurity requirements. These include:
  - Financial sector – Regulated by Monetary Authority of Singapore (MAS)
  - Healthcare sector – Regulated by Ministry of Health (MOH)

CYBERSECURITY ACT 2018

- The Cybersecurity Act 2018 establishes a framework for the protection of critical information infrastructures ("**CIIs**") against cybersecurity threats
- The Chief Executive of the Cyber Security Agency of Singapore ("**CSA**") has been appointed as the Commissioner of Cybersecurity ("**CS Commissioner**").
- The CS Commissioner may designate a computer or computer system as a CII if he is satisfied that (a) the computer or computer system is located wholly or partly in Singapore, (b) necessary for the continuous delivery of an essential service, and (c) its loss or compromise will have a debilitating effect on the availability of the essential service in Singapore.
- The owners of CIIs will have various statutory duties under the Cybersecurity Act, including but not limited to, conducting cybersecurity audits and risk assessments (section 15), as well as to report cybersecurity incidents in respect of CIIs (section 14).

FINANCIAL SECTOR

- Banks and financial institutions licensed under the Banking Act (Cap 19) and the Securities and Futures Act (Cap 289) have to abide by MAS' Technology Risk Management Notices – i.e., Notice 644 on Technology Risk Management ("**Notice 644**") and Notice CMG-N02 on Technology Risk Management ("**Notice N02**"), which are legally binding.
  - Under Notice 644 (for banks under the Banking Act) and Notice N02 (for financial institutions under the Securities and Futures Act), banks and financial institutions have to (amongst others):
    - notify MAS as soon as possible, but not later than 1 hour, upon the discovery of a system malfunction or IT security incident, which has a severe and widespread impact on the bank's operations or materially impacts the bank's service to its customers; and
    - submit a root cause and impact analysis report to MAS within 14 days the incident

HEALTHCARE SECTOR

- Following the SingHealth breach in 2018, the Ministry of Health issued Cybersecurity Advisory 1/2019 on 7 February 2019, advising all licensees under the Private Hospitals and Medical Clinics Act (Cap 248) ("**PHMCA**") to review the recommendations and cybersecurity best practices of the SingHealth Commission of Inquiry (COI), and to implement relevant measures where appropriate. These include:
  - Policy, governance and training issues, such as viewing cybersecurity as a risk management issue, and not merely an IT issue;
  - Protection and detection measures, such as putting in place safeguards (e.g. anti-virus security software) to protect electronic medical records); and
  - Response and recovery measures, such as engaging IT security service providers to provide cybersecurity response and recovery services

OVERVIEW OF DATA BREACH MANAGEMENT

- In this digital age, with the increased harnessing of personal data as a resource, data breaches should be viewed as inevitable.
- Data breach management should thus be seen as a risk management issue, and not merely an IT technical issue.
- Each organisation should have the appropriate expertise to properly respond to a data breach incident, which requires having either trained in-house IT personnel or external professional cybersecurity consultants.

DATA BREACH MANAGEMENT PLAN

- Organisations should put in place a data breach management plan, including the appropriate procedures for its employees to execute when a data breach occurs.
- This should include:
  - **A clear explanation of what constitutes a data breach (both suspected and confirmed)**: this allows employees to identify a data breach and respond promptly should one occur
  - **Procedures to report a data breach internally**: when an employee becomes aware of a potential or real data breach, he or she should know how and who to report the data breach to within the organisation
  - **Designation of a data breach management team**: organisations should appoint personnel trained in data breach management to a data breach management team. If organisations do not possess the appropriate expertise, they may send personnel for training, or seek the advice of professional data protection consultants.

DATA BREACH MANAGEMENT PLAN

- This should include:
  - **Responding to a data breach**: organisations should set out procedures to be taken in the aftermath of a data breach by the organisation's data breach management team.
    - Remedial actions to be taken
    - Notification of breach to PDPC and/or the individuals involved

WHEN A BREACH OCCURS

- Four key steps:
  - Containment
  - Assessment
  - Notifying of the Breach
  - Evaluation

WHEN A BREACH OCCURS - CONTAINMENT

- The first step is to contain the data breach to prevent further compromise of personal data.
- Organisations should act swiftly to take immediate measures to contain the data breach as soon as the data breach is confirmed, or even if it is merely suspected.
  - If the breach is discovered by an employee of the organisation, the data breach management team should be informed immediately
- The data breach management team should make an initial assessment of the data breach/suspected data breach, and should notify other key stakeholders, including internal and external legal counsel specialising in data protection and technical forensics specialists to be ready, so that their expertise will be available on short notice.

WHEN A BREACH OCCURS - CONTAINMENT

- The initial assessment of the data breach should assess the severity of the data breach, and should include an assessment of the following:
  - Cause of the data breach
  - Whether the data breach is ongoing
  - Type(s) of personal data involved
  - The affected systems and/or services
  - Whether help is required to contain the breach
- If the data breach occurs to a data intermediary, the data intermediary should report the data breach to the data controller without undue delay from the time it first becomes aware of the breach.

WHEN A BREACH OCCURS - CONTAINMENT

- Once the initial assessment has been done, organisations should consider taking the following immediate actions, where appropriate:
  - In the event of a data breach from an online system, isolating the compromised system from the Internet or network, or shutting down the compromised system if necessary
  - Immediately preventing further unauthorised access to the system. This may include resetting passwords if accounts and passwords have been compromised
  - Isolating the causes of the data breach in the system, and where applicable, securing access rights to the compromised system

WHEN A BREACH OCCURS - CONTAINMENT

- Organisations should also stop the practices that led to the data breach, and establish whether the lost data can be recovered and steps that can be taken to minimise harm or impact caused by the data breach.
- Organisations should consider alerting (a) the Police, if criminal acts are suspected, and/or (b) the Cyber Security Agency of Singapore, if the data breach is due to a cybersecurity attack, as these agencies may be able to assist with containing the data breach.
- Assessment of the data breach should be on an ongoing basis, until all relevant information relating to the breach has been considered. The initial data breach assessment should be revised accordingly, if subsequent findings uncover further facts.
- All steps taken, together with appropriate timestamps, should be dutifully recorded down to assist with follow-up investigations.

WHEN A BREACH OCCURS – ASSESSMENT

- Once the breach has been contained, organisations should conduct an in-depth assessment of the data breach – particularly, the extent and likely impact of the data breach.
- This will allow organisations to take appropriate steps to limit the impact of a data breach, as well as to assess if the PDPC and/or the affected individuals should be notified.

WHEN A BREACH OCCURS – ASSESSMENT

- In assessing the likely impact of the data breach, the organisation should consider the following:
  - **Context of the data breach**: Was the personal data leaked "sensitive"? Was the personal data publicly available before the breach? Were there NRIC numbers, health records or financial information leaked? Was the personal data of any minors leaked? These are issues that organisations must consider in determining the likely impact of the data breach.
  - **Ease of identifying individuals from the compromised data**: The impact may not be as great if individuals cannot be identified from the compromised data. For example, a compromised dataset of customer records containing full names and NRIC numbers would impact the affected individuals more than a dataset containing the age group of the affected individuals in bands.
  - **Circumstances of the breach**: Organisations should consider if data was illegally accessed and stolen by those with malicious intent, which may result in more significant harm if the personal data is sold on online black markets.

WHEN A BREACH OCCURS – ASSESSMENT

- Organisations should then come to a conclusion as to whether the data breach is likely or unlikely to result in significant impact or harm to the affected individuals.
- Organisations should also consider if it is necessary to take steps to reduce any potential harm to affected individuals. This may include offering counselling services, as well as engaging data security experts to monitor the Internet (including the dark web) for indications that the data may have been inappropriately used.

WHEN A BREACH OCCURS – NOTIFYING OF THE BREACH

- As discussed before the break, organisations will then have to make an assessment as to whether to notify PDPC and/or the affected individuals of the data breach.
- In addition notifying PDPC and/or the affected individuals, organisations should consider notifying the Police by lodging a police report, if criminal activity is suspected, and if this was not done earlier as part of the containment process.

WHEN A BREACH OCCURS – EVALUATING THE BREACH

- The final step is for the organisation to evaluate its response to the breach, especially if containment efforts and initial remedial actions were ineffective and more lapses are found
- If there are further lapses found, the organisation should consider implementing further remedial actions, to reduce the harm and/or potential harm to individuals

WHEN A BREACH OCCURS – EVALUATING THE BREACH

- Organisations should review and learn from the data breach, and consider the following areas:
  - Data breach management – are there ways to improve?
  - Existing measures and processes – are existing measures sufficient? Was there any blind spot that should be fixed?
  - Roles of external vendors – was the breach due to an external vendor? If so, are there sufficient contractual measures in place for the handling of personal data?
  - Management issues – was senior management equipped to manage the data breach? Was there sufficient/effective direction given in managing the data breach?
  - Employee issues – were employees aware of security related issues, and trained on personal data protection measures?

DREW & NAPIER