Privacy Interviews with Experts
September 2015

Eugene Low
Partner
Hogan Lovells
Hong Kong

Data breach notification in Hong Kong: Why is it important for companies?

The number of data breaches is rapidly increasing not only in Hong Kong but around the world, so it is critical for companies to be prepared to prevent and handle these situations.

In this interview, Mr. Low provides great insight on best practices for responding to a data breach, including immediate notification to affected individuals and to the Privacy Commissioner among others, what needs to be included in a data breach notification and how it should be communicated.

Eugene Low is a well-rounded practitioner handling all areas of contentious and advisory IP, TMT and data privacy work in Hong Kong and China. Eugene advises extensively on data privacy compliance, data breaches and is experienced in advising clients in handling customer complaints and investigations by regulatory authorities. Mr. Low is an accredited mediator and a member of the INTA Bulletins Committee. He also serves as a panellist for the Hong Kong International Arbitration Centre, the Asian Domain Name Dispute Resolution Centre and the Kuala Lumpur Regional Centre for Arbitration.
Eugene is also a regular contributor for various publications and also a frequent speaker on data privacy issues.

Nymity: What are the most common causes of data breaches in Hong Kong?

Eugene: As in other jurisdictions, data breaches in Hong Kong can happen for many reasons. In recent years, however, the most common causes appear to be poor IT security and the lack of employee awareness. As examples, in its latest annual report, the Privacy Commissioner of Hong Kong highlighted two data breach incidents in 2014, both of which were attributed to one or both of these causes:

Case #1: A university reported that its network-attached servers had been hacked and files containing personal data of more than 15,000 individuals had been accessed by a hacker. The university responded to the Privacy Commissioner's enquiries that the incident was caused by lack of proper security patches on the servers, hence allowing hackers to use ransomware to exploit the security loophole.

Case #2: A university reported that a staff member had mistakenly sent an invitation email for admission activities to over 3,000 former students. The mistake was due to human error in conducting a mail merge, resulting in a mismatch in the recipients' data.

Nymity: Is it mandatory for a company to provide notification in the event of a data breach?

Eugene: No. The Privacy Commissioner however encourages companies to consider notifying the individuals concerned and other relevant parties (e.g. the Privacy Commissioner, law enforcement agencies, etc.) when a real risk of harm is reasonably foreseeable.

Nymity: What legal provisions or advisory guidelines apply to the notification of data breaches in Hong Kong?

Eugene: There are no legal provisions which apply to data breach notifications in Hong Kong. A number of advisory guidelines are applicable, notably the Guidance Note on "Data Breach Handling and the Giving of Breach Notifications" published by the Privacy Commissioner as well as various circulars and guidance notes issued by the Hong Kong Monetary Authority applicable primarily to the banking sector.

Nymity: In the event of a data breach:

- **How can the risk of harm be assessed?**
- **Who must assume the responsibility of handling the incident within the company?**
- **To whom should this person notify the data breach? Is there any difference between the notification to the regulator and the one to customers?**
- **What is the time framework to make a notification?**
- **How can a notification be done?**
- **What should be included in the notification?**

Eugene: As mentioned, there are no legal provisions on data breach notifications in Hong Kong. However, as a matter of good practice:

- **How can the risk of harm be assessed?**

  Risk-assessment and fact-finding is a crucial first step. Ideally, all the relevant stakeholders (both internal and external) should be involved as soon as possible. However, given the prevalence of data breaches happening in the cyberworld, in terms of priority, it is almost inevitable that the company's IT personnel would have to be involved to identify the cause of the breach and to implement remedial measures. It is still relatively uncommon for companies in Hong Kong to have a designated personal data officer (or very often they wear multiple hats) so marketing and legal teams will also play a crucial role in identifying the data/individuals concerned and the associated risks.

- **Who must assume the responsibility of handling the incident within the company?**

The company should have an incident-response team consisting of the various stakeholders, e.g. IT, legal, marketing, public relations, human resources. The team should have a co-ordinator but in reality the team members do have to work very closely together because a data breach very often involves a matrix of issues to be assessed and dealt with.

- **To whom should this person notify the data breach? Is there any difference between the notification to the regulator and the one to customers?**

  In most cases, the primary classes of persons to be notified would be the affected individuals and the Privacy Commissioner. In appropriate cases, notifications may also be made (or have to be made) to law enforcement agencies (for example where criminal activities are suspected) or to industry associations or regulators (for example, the financial industry regulators).

  Notifications may also be made to the public at large, for example by posting a data breach notification on the data user's website (this would be appropriate if, for instance, the data user wants to notify the data subjects affected but cannot identify them or their contact information), or to Internet service providers/search engines if assistance is required for removing caches. Some data users may opt to make a notification to enhance transparency and to convey a message that they have taken and will take steps to safeguard their customers' personal data.

- **What is the time framework for notification?**

  If the company decides to make a notification, this should be done as soon as possible. Data breaches are usually time-sensitive. Delay in making notification may result in further damage to the individuals (e.g. further misuse of their data) and to the company (e.g. loss of credibility).

- **How should notification be done?**

  This depends. As mentioned above, companies who want to be more transparent may choose to make the notification by posting a message on their official website. There have been recent examples in Hong Kong where a company notified its loyalty scheme members of a suspected hacking by way of a newspaper notice, and where a bank wrote to the affected customers individually of a suspected leak of credit card details. In the latter case, it would not have been appropriate for the bank to make a public notification as this might lead to further loss to its customers.

- **What should be included in the notification?**

  Usually a notification will include:

  - Cause and extent of the breach
  - Immediate remedies that the company has taken
  - Long-term remedial measures
  - In appropriate cases, companies may offer an apology or a sweetener (e.g. in the form of a coupon)

  The key message to send out is that the company has taken the right steps which will minimise the chances of a repeat incident.

Nymity: Are there any exemptions to notification e.g. breaches involving encrypted data?

Eugene: As notifications are not mandatory in Hong Kong, there are not really any exemptions. However, for example for breaches involving encrypted data, the company, after having assessed the risk, may come to the conclusion that the chances of real loss are low and therefore may opt not to make a notification at all.

Nymity: What are the consequences for failing to provide notification? What powers does the regulator have in respect of enforcement in the event of non- disclosure?

Eugene: Generally speaking, there are no legal consequences as such for failing to give notification for a data breach in Hong Kong (but there can be legal risks where the company's non-disclosure may arguably lead to further loss suffered by the individuals, e.g. stolen credit card details), and the Privacy Commissioner does not have any power of enforcement in the event of non-disclosure. One potential downside of non-disclosure is that if the breach does come to light, negative publicity may follow and the company may be perceived as trying to conceal its fault both in the eyes of its customers and the Privacy Commissioner.

Nymity: What lessons can a company learn from a data breach to prevent recurrence?

Eugene: I would suggest that companies take a step back to conduct a complete review of their data privacy practice and policy. The whole concept of data security relates back to the fundamentals of data privacy. For instance, before collecting personal data, companies should critically ask themselves how much personal data do they really need to collect? How long do they need to keep those data for? Where are those data kept? It is notable that a lot of data breach cases involve the leak of irrelevant or obsolete personal data which arguably add to the damage rather unnecessarily.

Nymity: What are the top five data breach notification best practices that companies operating in Hong Kong should implement?

Eugene: While there is no "one-size-fits-all' solution, generally speaking I would recommend companies in Hong Kong to pay attention to the following:

- Develop a data breach response policy. Having an established policy (as opposed to handling a data breach on an ad-hoc basis) would help companies in pulling together the relevant stakeholders (both internal and external), and assessing the steps that ought to be taken, much more efficiently and consistently.

- Take a wholesale review of the company's data privacy practice and policy. Avoid keeping obsolete, unnecessary personal data – this will in turn reduce the company's exposure to data breaches.

- Make sure the IT infrastructure (in particular security measures) is reasonably up-to-date.

- Provide regular data privacy training and guidance to employees, contractors and data processors. Develop appropriate data security-related manual, e.g. BYOD and social media policies.

- Consider taking out cyber liability insurance.