Data Privacy Asia
SINGAPORE 2016

To breach, or not to breach

An update on data breach in Hong Kong

Charmaine Koo
Partner at Deacons

Building Digital Trust:
Establishing an Ecosystem of Trust and Protection in the Digital Age

November 9–11, 2016

Charmaine Koo

- Co-head of Intellectual Property Department
- Head of IP Commercial & Litigation team
- Practice covers all areas of IP as well as entertainment, personal data (privacy), technology, and advertising

Data Privacy Asia
SINGAPORE 2016

Outline

- Global data security crisis
- Hong Kong position regarding data security?
- What are the legal requirements in relation to data security and breach?
- Practical steps for handling data breaches
- Cases examples

Global Data Security Crisis

- Unprecedented risks

  ↑ Digitisation

  ↑ Globalisation → storage anywhere in cyberspace

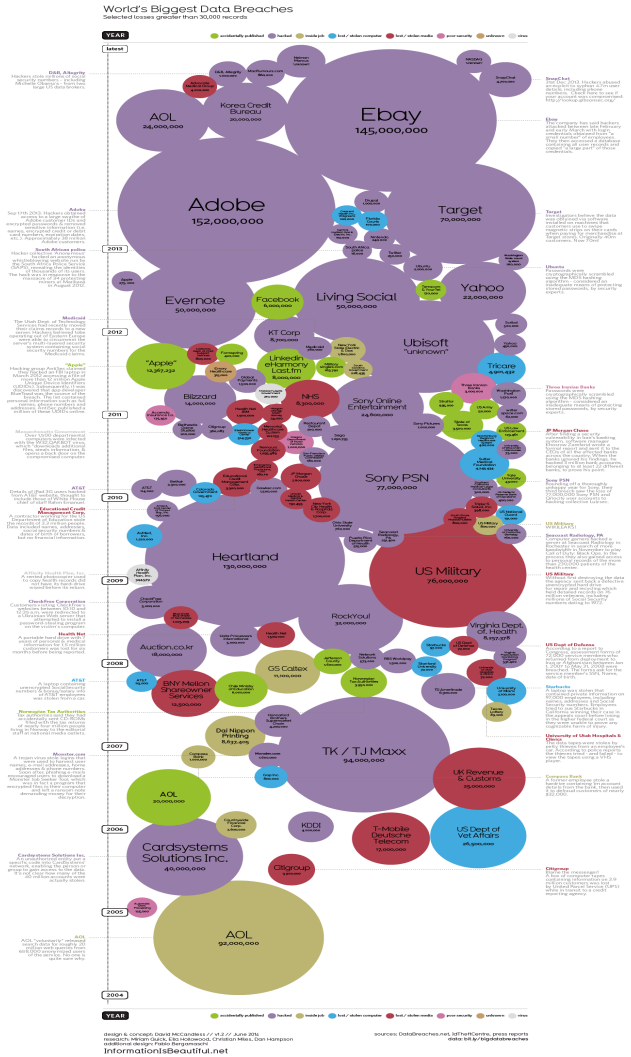
  ↑ Collection of massive amounts of data

  ↑ Hacking and difficulty in tracking hacker in cyberspace

Global Data Security Crisis

Data Breach = Serious Problem

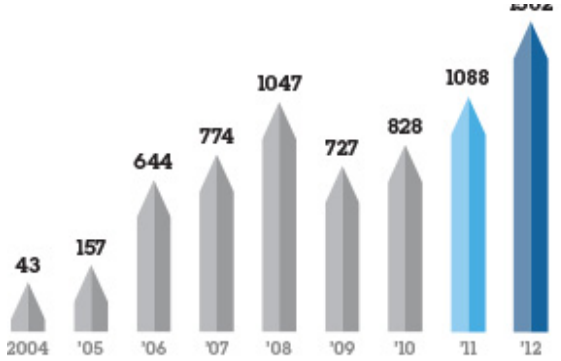
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-static/



Source: http://www.informationisbeautiful.net

Data Privacy Asia
SINGAPORE 2016

IBM Statistics



38%

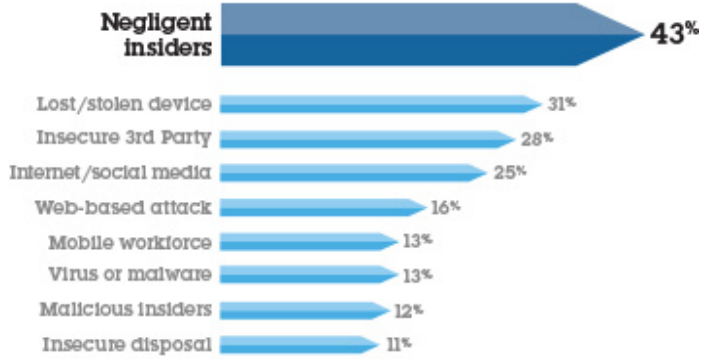
increase in incidents of loss, theft and exposure of personally identifiable information over the last year

Learn more

43%

of C-level executives say negligent insiders are the greatest threat to sensitive data

Learn more



75%

of companies say IT risks impact customer satisfaction and brand reputation

Learn more

Source: https://www-935.ibm.com

Hong Kong Problem

Record number of public complaints:

- 2015 – 871,000 HK individuals affected by data breach (47,000 in 2014)
- 2015 – 98 incidents reported re loss of data, hacking, disclosure (70 in 2014)
- 1 in 8 Hong Kong individuals affected by data breach in 2015
- Aggressive enforcement by Privacy Commissioner and Police

University of Hong Kong's medicine department 'sorry' for patient data breach

Laptop containing personal information of more than 3,600 patients believed to have been stolen; police are investigating

Hong Kong's top medical school has expressed its "deepest apologies" after a laptop computer containing the personal data of more than 3,600 patients was suspected to have been stolen, causing a massive data breach.

Source: http://www.scmp.com

Data breach at Hong Kong toy maker VTech highlights broader problems

The theft of toy maker VTech Holdings' database highlights a growing problem with basic cyber security measures at small, non-financial companies that handle electronic customer data, industry watchers said on Monday.

Source: http://www.cnbc.com

Global Concern and Stepping Up Penalties & Requirements

- Mandatory Breach Notification to Authorities:

Countries WITH general data security breach notification requirement	Austria, Canada (only Alberta), Colombia, Germany, Hungary, Italy, Japan, Mexico, The Netherlands, South Korea, Taiwan, United States (46 out of the 50 states, plus District of Columbia)
Countries WITH data security breach notification requirement only on providers of electronic communications/ telecommunications services	European Union, France, Spain, United Kingdom
Countries WITHOUT data security breach notification requirement	Australia, Belgium, Brazil, Canada (other than Alberta), Denmark, Hong Kong, Israel, Malaysia, Russia, Singapore, Switzerland

Global Concern and Stepping Up Penalties & Requirements

- Increased Requirements:
  - New General Data Protection Regulation (GDPR) of the EU(effective 25 May 2018) of the EU:
    - notification within 72 hours
    - administrative fine of up to €10 million or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher
  - Australia Privacy Amendment (Notice of Serious Breaches) Bill published late 2015:
    - Mandatory notice "as soon as practicable"
    - Fine A$1.8 million

Hong Kong: What are the legal requirements for data security?

- Hong Kong Personal Data Privacy Ordinance (PDPO)
- Data Protection Principle 4
  - A data user must take **all practicable steps** to ensure that personal data held by a data user are protected against unauthorised or accidental access, processing, erasure, loss or use having particular regard to:
    - the kind of data and the harm that could result if any of those things should occur;
    - the physical location where the data is stored;
    - any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;
    - any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and any measures taken for ensuring the secure transmission of the data.

Hong Kong: What are the legal requirements for data security?

- Data Protection Principle 4
  - If a data user engages a "data processor" (i.e. a person who processes personal data on behalf of another person, and does not process the personal data for any of the person's own purposes), whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user **must adopt contractual or other means** to prevent:
    - any personal data transferred to the data processor from being kept longer than is necessary for processing of the data; and
    - unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing

What are the Legal Requirements in Relation to Data Breach in HK?

- No specific legal requirements under PDPO what to do when breach
- No mandatory reporting obligation
- Wording in DPP 4 "take all practicable steps" to ensure data protected – not absolute
  - Depends on list of factors eg. Kind of data and importance of data

What are the Legal Requirements in Relation to Data Breach in HK?

- Breach of DPPs:
  - No immediate penalty
  - Investigation by Privacy Commissioner (PC)
  - Enforcement Notice from PC
  - If Enforcement Notice not complied with:
    - Max fine HKD50,000 (USD6500)
    - Max imprisonment 2 years
  - Civil action by data subject for damages suffered (incl. injury to feeling)

Guidance Note on Data Breach handling and the Giving of Breach Notifications (October 2015)

- Not legally binding but good indication as to how PC approach and interpretation
- "Data Breaches" include:
  - Loss of PD kept in storage eg. Laptops, USB, paper files etc.
  - Improper handling of PD eg. Sending to wrong party, unauthorised/mistaken access by employees etc.
  - Hacking of database by outsiders
  - Disclosure of PD through deception
  - Leakage of data by installation of file-sharing software

Practical Steps to handle a Data Breach

4 Steps Process:

Step 1: Promptly gather essential information:

- How did the breach occur?
- Where did the breach take place?
- How was the breach detected and by whom?
- What was the cause of the breach?
- What kind and extent of PD involved?
- How many data subjects were affected?

Practical Steps to handle a Data Breach

Step 2: Contacting interested parties and adopting measure to contain the breach:

- Depending on breach:
  - Law enforcement agencies eg. Police
  - Regulators eg. Privacy Commissioner, HK Monetary Authority
  - Internet service providers
  - IT Experts for reporting, advice and assistance
  - Lawyers?

Practical Steps to handle a Data Breach

Step 2 (Cont'd) : Adopting measure to contain the breach:

1. Stopping system involved
2. Changing user's password and system configurations to control access and use
3. Consider internal or external technical assistance to remedy system loophole and stop hacking
4. Cease or change access rights of suspected persons
5. Notify law enforcement authorities if theft or criminal activities suspected
6. Keeping evidence to facilitate investigation
7. Contact data processor (if involved) and take immediate remedial actions

Practical Steps to handle a Data Breach

Step 3: Assessing the Risk of Harm:

- What are the potential damages?
  - Threat to personal safety
  - Identity theft
  - Financial loss
  - Humiliation, loss of dignity, damage to reputation/relationship
  - Loss of business and employment opportunities
- Actions to be taken depends on specific facts:
  - Kind of data leaked: Sensitive data?
  - Amount of data involved

Practical Steps to handle a Data Breach

Step 3 (Cont'd): Assessing the Risk of Harm:

- Circumstance of breach? eg. Online difficult to trace recipient and not traceable
- Likelihood of identity theft or fraud eg. Credit card details, ID car, bank details
- Whether leaked data adequately encrypted, anonymised or otherwise rendered inaccessible eg. Password protected
- Ongoing or risk further exposure?
- Isolated incidence or systematic problem? eg. One-off human error
- If physical loss, whether recovered data before accessed/copied?
- Effective mitigation/remedial measures taken after breach?
- Reasonable expectation of privacy of data subjects?

e.g Low risk if USB with encrypted data with no sensitive data is lost and found

Practical Steps to handle a Data Breach

Step 4: Consider Giving Data Breach Notification to Data Subjects:

- No legal requirement to notify data subjects or Privacy Commissioner under the PDPO – but may be beneficial?
- Guidance Note suggests data users adopt a system of notification in handling a data breach. Notification might include:
  - formation about the incident
  - a description of the personal data involved
  - an account of the remedial steps taken by the data user
  - what the data user can do to assist the data subjects
  - what the data subjects can do to protect the data and mitigate potential damages
  - a person to contact and useful addresses

Practical Steps to handle a Data Breach

Step 4: Breach Notification:

- However, whether or not a notification should be made may depend, for example, on whether:
  - such notification may, in fact, increase the risk of harm to data subjects
  - data subjects are not identifiable immediately, or where public interest exists, in which public notification (such as through a website or media) may be more effective (again bearing in mind whether such method of notification adopted might increase the risk of harm)
  - whether any law enforcement agencies have, for investigative purpose, made a request for a delay

Data breaches – Case Example

HKA Holidays Limited Leaked Customers' Personal Data through the Mobile Application "TravelBud" (R14-6453)

- Mobile app "Travelbud" of Hong Kong Airline ("HKA")
- 2013 Sept – Data breach notification
  - Personal data of 6 customers leaked through IOS platform
    - Name, ID / Passport, Tel, email, DOB
- Investigation
  - Outsourced development and maintenance of App to PRC developer
  - Data stored in server in BJ
    - Not encrypted except for login password

Data Breach – Case Example

- DPP4
  - Take all reasonable practicable steps to ensure data protected against unauthorized or accidental access
  - Not absolute guarantee
- Problem arise due to Apple's launch of new iOS7
  - Block reading by apps of MAC address as mobile device ID
  - Now give one fictations MAC address for all iOS7 users
  - Leaked user's data to other users
- PRC service provider admitted did not update App despite Apple's 3 months advance notice
- Service provider not data user
  - No control over collection, holdings, processing or use

Data Breach – Case Example

- S. 65(2) ∴ HKA remains accountable

  ➔ breached DDP4(1)

  – Upon customer complaint HKA
    - Immediately suspend affected function
    - Duly notified all affected individuals
    - Sent data breach notification to PC
    - Released updated version – deleted function
    - No more complaints
  – No Enforcement Notice → only warning

Data Breach – Case Example

- **VTech Breach: Reputational Damage**
  - Vtech is a HK based developer of toys including sells children's tablets, downloadable children's games, books and other educational content
  - Nov 2015 data breach: data of some 5 million parents and 6 million children were taken in the VTech attack
  - Vtech's stock has fallen 22 percent, shares were suspended on day of announcement of breach and trade in other VTech securities has also been suspended
  - Privacy Commissioner investigation
  - Negative media reports

Data Breach – Case Example

AND THEN as part of Vtech's response for data breach…

- Vtech went and amended its T&C to shift liability to customers:

> *"You acknowledge and agree that any information you send…may not be secure and may be intercepted and later acquired by unauthorized parties…. Recognising such, you understand and agree that…neither Vtech nor its suppliers … will be liable to you for any direct, indirect, incidental…. Or other damages of any kind…"*

VTech shifts data breach liability to customers - why this is a non-starter

VTech's clever defence against data breaches - shift liability to the customer.

Source: http://www.computerworlduk.com

VTech not backing down on terms change after data breach

Despite widespread public condemnation, Hong Kong toy maker VTech is not backing down from a change in its Terms and Conditions, ducking responsibilities in the event of a breach.

"Companies should spend more time actually protecting themselves from attacks, instead of trying to protect themselves against liability."

- John Gunn, spokesman for security vendor VASCO Data Security

"Parents are continuing to post sarcastic comments on the company's social media site, keeping up the pressure."
"Real great of you, disgusting business, putting our children in harms way!"

"Frankly, its just plain lazy, and obviously no substitute for a competent data security program."

- Jeff Hill, channel marketing manager at security vendor STEALThbits Technologies

Source: http://www.csoonline.com

2014 Global survey by SafeNet Inc. across world's largest economy shows that 2/3 of respondents would never, or were very unlikely to shop or do business again with a company that had experienced a data breach involving financial data.

Good Data Breach Handling Makes Good Business Sense:

- Reduce risk of issuance of enforcement notice
- Minimize reputational risks
- Often the most damaging even if there is no legal consequence
- Show company's responsible and accountable attitude
- Assurance to customers
- Regain goodwill and business relationship and public confidence

Data Privacy Asia

SINGAPORE 2016

Building Digital Trust: Establishing an Ecosystem of Trust and Protection in the Digital Age