

Seminar on Cyber Security and Personal Data Privacy Protection in eHRSS
24 January 2019 | Prince of Wales Hospital

Data Breaches and Cybersecurity

保護・尊重個人資料
Protect, Respect Personal Data



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Evolution of Data

2



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong



港國圖國
WATERFRONT SOUTH

明日公開發售共188個單位

由電腦抽籤排列揀樓次序之

| 申請表號碼 | 揀樓次序 | 身份證號碼／商業登記證號碼 |
|--------|-------|---------------|
| SA0808 | 00764 | D670151(6) |
| SA0809 | 00701 | D394775(J) |
| SA0810 | 00475 | D433676(4) |
| SA0811 | 00559 | K185665(A) |
| SA0812 | 00153 | D525178(0) |
| SA0813 | 00871 | G285170(8) |
| SA0814 | 00891 | G080280(7) |

售樓處設在「銅鑼灣世貿中心25字樓」
並於明日上午10時正開售，敬請留意！

PCPD



PCPD.org.hk

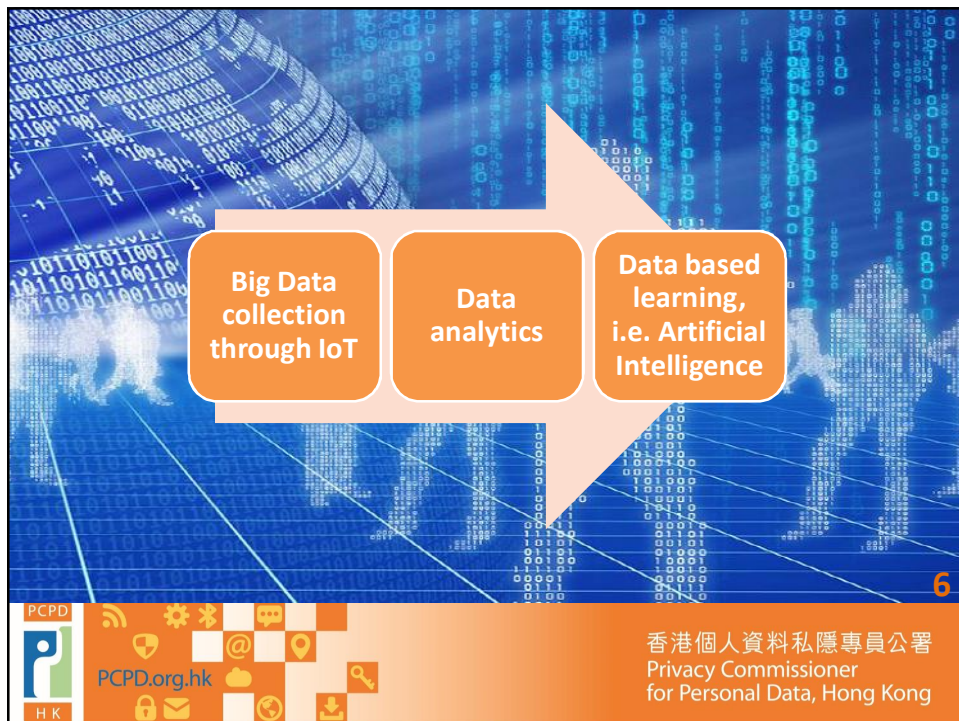
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Internet of Things

PCPD

PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong



“Information is the oil of the 21st century, and analytics is the combustion engine.”

(Peter SONDERGAARD – Gartner)

Source: DataWorks Summit/ Hadoop Summit

7



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

How much is your data worth?

| Category | Price |
|--|------------------|
| Music Streaming Account | \$2.75 |
| Movie Streaming Account | \$2.75 |
| TV Shows Steaming Account | \$1.00 - 3.00 |
| Payment Credentials | \$1.50 |
| Social Security Number | \$1.00 |
| Driver's License | \$20.00 |
| Credit Card | \$8.00 - \$22.00 |
| Email Address & Password | \$0.70 - \$2.30 |
| Medical Record from Large Scale Attack | \$1.50 - \$10.00 |
| Complete Medical Record | Up to \$1,000.00 |

Source: <https://keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html>

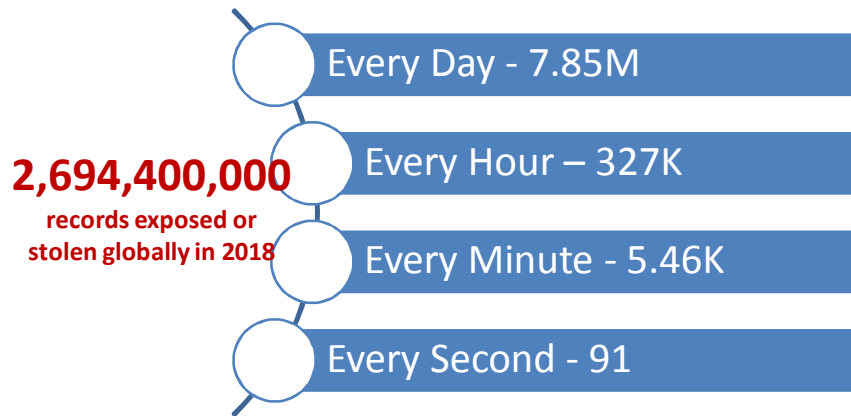
8



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Figures of Data Breach in 2018



Sources: Bloom & Identity Theft Resources Centre

9



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Recent Data Breach Incidents

| Companies involved | Number of affected subjects |
|------------------------|-----------------------------|
| Marriott International | 383,000,000 |
| Twitter | 330,000,000 |
| My Fitness Pal | 150,000,000 |
| Facebook | 147,000,000 |
| Quora | 100,000,000 |
| Firebase | 100,000,000 |
| My Heritage | 92,000,000 |
| Uber | 57,000,000 |
| Ticket Fly | 27,000,000 |
| Google+ | 500,000 |
| British Airways | 380,000 |

10



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong



The diagram illustrates the evolution of cybercriminals. It features a central figure of a cybercriminal in a white suit and hat. Surrounding this figure are several icons: a document with a person icon and the word 'IDENTITY', a money bag with a dollar sign, a warning triangle with an exclamation mark, a tombstone with 'RIP', and a smartphone with 'Rx'. Blue arrows indicate a cycle of progression from the cybercriminal to identity theft, then to financial gain, then to a warning, then to a tombstone, and finally back to the cybercriminal. The background is a blue globe.

Evolution of Cybercriminals

11

PCPD
HK

PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong



The slide features a background image of the Hong Kong skyline with the Victoria Harbour and mountains in the distance. The title 'Personal Data (Privacy) Ordinance' is prominently displayed in the center.

Personal Data (Privacy) Ordinance

PCPD
HK

PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

What is “Personal Data”?



(a) relating directly or indirectly to a living individual

(b) practicable for the identity of the individual to be directly or indirectly ascertained

(c) in a form in which access to or processing is practicable



PCPD.org.hk

13

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

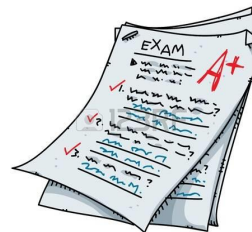
Personal Data?



Gossip



Fingerprint



Exam questions
and answers

14



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

6 Data Protection Principles

收集目的及方式
Collection
Purpose & Means

1



保安措施
Security

4



準確性、儲存及保留
Accuracy & Retention

2



透明度
Openness

5



使用
Use

3



查閱及更正
Data Access &
Correction

6



15



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

4. Data Security Principle



Data user shall take all practicable steps to ensure that personal data held by them are protected against unauthorised or accidental access, processing, erasure, loss or use.

16



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

What is “all practicable steps”?



17



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

What is “all practicable steps”?



Personal data privacy protection as part of the corporate governance responsibilities, covering business practices, operational processes, policies and training

Comprehensive and on-going review and monitoring process; build a robust privacy infrastructure

1. General and Organisational Preventive Measures

Open and transparent information privacy policies and practices

Top management commitment, a top-down business imperative throughout the organisation

18



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong



What is “all practicable steps”?

2. Technical Security Measures

Hardware security, e.g. information system, network infrastructure, etc

Policies and procedures for regular review of security systems

Security measures and steps for system login, data transmission and storage, and adoption of international standards and technology, e.g. hashing, encryption, etc

19

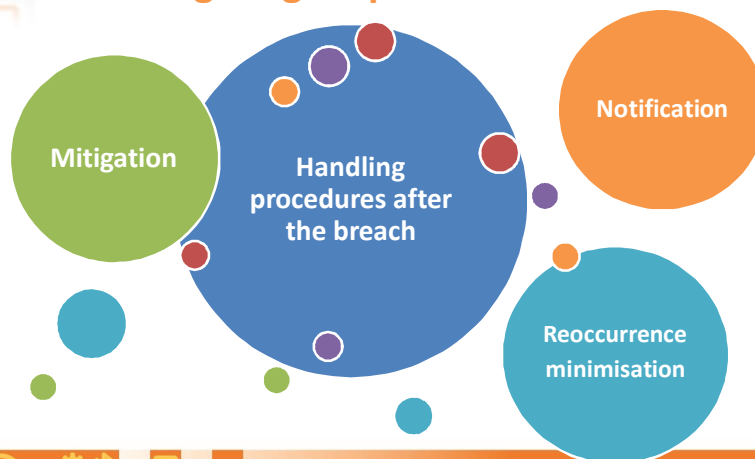


香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong



What is “all practicable steps”?

3. Mitigating Steps after the Breach



20



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong



What is “all practicable steps”?

4. Other Considerations

Nature, size and resources of the data user

Likelihood of adverse consequences for affected individuals

Complexity of its operations of the data user and its business model

Amount and sensitivity of personal data held



21



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong



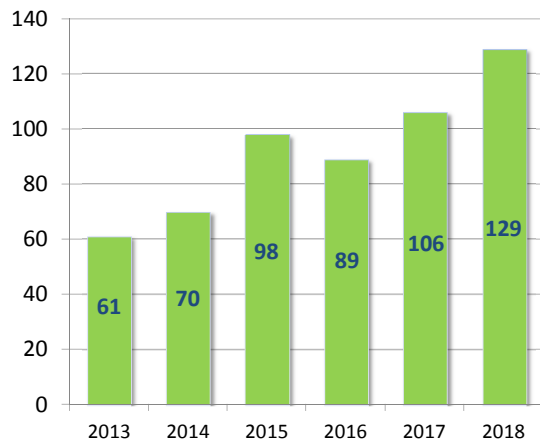
Data Breaches

22



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Data Breach Notifications Received



| Year | No. of Data Subjects Involved |
|------|-------------------------------|
| 2013 | 90,000 |
| 2014 | 47,000 |
| 2015 | 871,000 |
| 2016 | 104,000 |
| 2017 | 3,866,000 |
| 2018 | 2,387,000 |

23



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Common Types of Data Breach Incidents

1. loss of physical documents or portable device

2. IT systems with improper settings or being attacked by hackers or malwares

3. missent of emails or letters

4. employees' non-compliance with data security policy

5. improper disposal of personal data

24



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Cases in Medical Sector



CASE 1

- scrap paper was used for printing appointment slips and distributed to a patients
- other patients' personal data were shown on the back of the appointment slips

CASE 2

- an external component (with patients' personal data saved in it) of an apparatus in a hospital was stolen
- the device was not locked by a chain lock
- no change of the log-in password default upon manufacture

密碼*****

25



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Cases in Medical Sector

CASE 3

- hospital waste containing patients' personal data were found abandoned on the street outside a shredding factory which was a service provider of the hospital



26



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Data Security in eHRSS

- Ensure that when authorised staff log into the eHRSS, eHR shown on the computer screen will not be seen by unrelated third parties.
- Keep the eHR downloaded or printed from the eHRSS safely.
- Guidelines on the use of portable storage devices should be formulated to avoid leakage of personal data.
- Adopt appropriate measures to ensure that healthcare providers' data systems are adequately safeguarded and properly functioned.



27



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

How to report a data breach to PCPD

https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html

About PCPD | Data Privacy Law | News & Events | Compliance & Enforcement | Complaints | Legal Assistance | Education & Training | Resources Centre | Enquiry

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Home > Compliance & Enforcement > Data Breach Notification

Compliance & Enforcement

Commissioner's Findings
Court Judgment
Administrative Appeals Board's Decisions
Case Notes
Data Breach Notification
Submissions on Privacy Issues
Consultations

Data Breach Notification

A data breach is generally taken to be a suspected breach of data security of personal data held by a data user, by exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use.

While it is not a statutory requirement on data users to inform the PCPD about a data breach incident concerning the personal data held by them, data users are nevertheless advised to do so as a recommended practice for proper handling of such incident. You may make reference to our "Guidance on Data Breach Handling and the Giving of Breach Notifications" before submitting a data breach notification.

For submitting a data breach notification to the PCPD, please click [here](#) to download the Data Breach Notification Form. You can then fill in the form by making reference to the "Notice" and "Information Notes" contained therein.

After completing the form, please submit it and other relevant documents concerning the data breach (if any) which you wish to provide by clicking the icon below and following the instructions.

Upload Data Breach Notification Form and other documents:

(At most 20MB in total)

Acknowledgement through email

- Please note that if your submission of the Data Breach Notification Form is successful, you will receive a confirmation notification. You may also choose to provide your email address here:
[Please Enter Email Address], so that the system can send an acknowledgement to your email address.
- Please input the verification code appearing in the picture on the right:
4 8 5 7

28



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

4 Steps for Data Breach Handling and Notifications

Step
1



Collecting Information Immediately

Immediate gathering of essential information relating to the breach including:

- When and 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 personal data was involved?
- How many data subjects were affected?

29



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

4 Steps for Data Breach Handling and Notifications

Step
2



Contacting the Interested Parties & Adopting Containment Measures

Interested parties may include:

- The law enforcement agencies
- The relevant regulators (e.g. Privacy Commissioner for Personal Data, Hong Kong (the “Commissioner”))
- The Internet companies
- IT experts

30



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

4 Steps for Data Breach Handling and Notifications



Assessing the Harm

Assessing the potential harm caused by a data breach, for examples:

- Threat to personal safety
- Identity theft
- Financial loss
- Humiliation or loss of dignity, damage to reputation or relationship
- Loss of business and employment opportunities

31



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

4 Steps for Data Breach Handling and Notifications



Considering the Giving of Notification

When real risk of harm is reasonably foreseeable in a data breach, the data user should consider:

- Notifying the affected data subjects and the relevant parties
- The consequences for failing to give notification

32



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Actions to be taken by PCPD

- PCPD would assess the information provided in the Data Breach Notification and consider whether a compliance check or compliance investigation is warranted



33



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Types of Cyber Attack

Code Injection

Phishing

Malware

Password
Cracking

34



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Incident 1: Customer databases and servers of a toy maker were hacked

BACKGROUND

- leaked personal data of about 5 million parents and 6.6 million related children
- data included parents' names, email addresses, children's names, gender, and full dates of birth; and chat and voice messages and photos



35



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Incident 1: Customer databases and servers of a toy maker were hacked

CAUSES

- no basic security measures: countermeasures to prevent SQL injections, installing web application firewalls, and encrypting personal data
- IT security policies and guidelines did not retroact upon old systems
- failed to monitor the implementation of its IT security policies and guidelines and update time timely

36



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Incident 1: Customer databases and servers of a toy maker were hacked

REMEDIAL ACTIONS

- stopped collecting the children's dates and months of birth during account registration
- enhanced its protective measures against unauthorised data access
- promulgated a new Data Security Policy
- formed a Data Security Governance Board



37



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Incident 2: Network-attached storage servers of a university were hacked

BACKGROUND

- files containing personal data of 15,547 patients and 200 students and/or staff were maliciously encrypted by a hacker
- the university was blackmailed for bitcoins in exchange for the decryption key



CAUSES

- lack of proper security patches on the servers → allowed the hacker to use ransomware to exploit the security vulnerabilities of some servers running older versions of the operating system

38



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Incident 2: Network-attached storage servers of a university were hacked

REMEDIAL ACTIONS

- setting up a new server following the university's guidelines on server protection
- performing regular maintenance on the new server
- identifying unprotected file servers used by the faculty, and protecting them behind its firewall
- conducting a departmental information security review
- reinforcing awareness of its departmental IT staff members of data security



39



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Incident 3: Customer databases of travel agencies were hacked

BACKGROUND

- databases of several travel agencies containing personal data of about 200,000 customers were encrypted by a hacker who demanded a ransom in exchange for decryption key

REMEDIAL ACTIONS

- enabling web application firewall
- adopting two-factor authentication for remote access
- encrypting the customer database
- creating an offline backup, conducting penetration testing and vulnerability scanning regularly, etc.



40



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Risks of Engaging Data Processors



Service providers (as data processors) may keep data longer than necessary [DPP 2(3)]

Request for data deletion ≠ Immediate deletion

41



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Risks of Engaging Data Processors



Unauthorised access to customer and business data (e.g. hacking, data breach) [DPP 4(2)]

42



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Risks of Engaging Data Processors



“Secondary uses” of data with or without data users’ knowledge
[DPP 3 & s.65(2)]

43



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Incident 4: Customers’ personal data of a bank was downloaded without authorisation

BACKGROUND

- a contractor downloaded 964 data files (with 210,000 customers’ personal data) from the bank’s computer workstation to his mobile device without authorisation
- measures implemented at the material time:
 - ✓ contractual control, confidentiality agreement
 - ✓ requiring the contractor to work in the bank office
 - ✓ data loss prevention system controls
 - ✓ monitoring tools to detect abnormal activities

44



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Incident 4: Customers' personal data of a bank was downloaded without authorisation

CAUSES

- misconfiguration of its data loss prevention system → failed to block the transfer of data from computer workstations to portable devices

REMEDIAL ACTIONS

- re-configuring data loss prevention system controls
- enhancing inadvertent data disclosure and end-point security tools
- monitoring external data transfers
- only dummy or masked personal data to be used for testing and system development



45



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Lesson Learnt to Prevent Recurrence



improvement of security



control of access rights



revision or promulgation of privacy policy and practice



effective detection of data breach



strengthening of monitoring and supervision



provision of on-the-job training

**LESSON
LEARNT** 46



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Privacy Issues in the Age of Big Data, Artificial Intelligence & Internet of Things

- convert data collection
- tracking and monitoring
- re-identification
- profiling, unfairness and discrimination
- low transparency
- unpredictability
- cybersecurity



47



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Privacy-based Solutions



48



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Promoting Data Ethics

Privacy Management Programme – Privacy Management Programme

*paradigm shift from compliance to
accountability*

Data ethics –

*ethical & fair processing of data – due
consideration of the rights, interests
and freedoms of individuals*



49



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

PCPD's Strategic Focus



50



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong



Contact Us



Copyright



This PowerPoint is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this PowerPoint, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.



- ☐ Website
- ☐ Email
- ☐ Tel
- ☐ Fax
- ☐ Address

www.pcpd.org.hk
enquiry@pcpd.org.hk
 2827 2827
 2877 7026
 Room 1303, 13/F,
 Sunlight Tower
 248 Queen's Road East
 Wanchai, Hong Kong

香港個人資料私隱專員公署
 Privacy Commissioner
 for Personal Data, Hong Kong