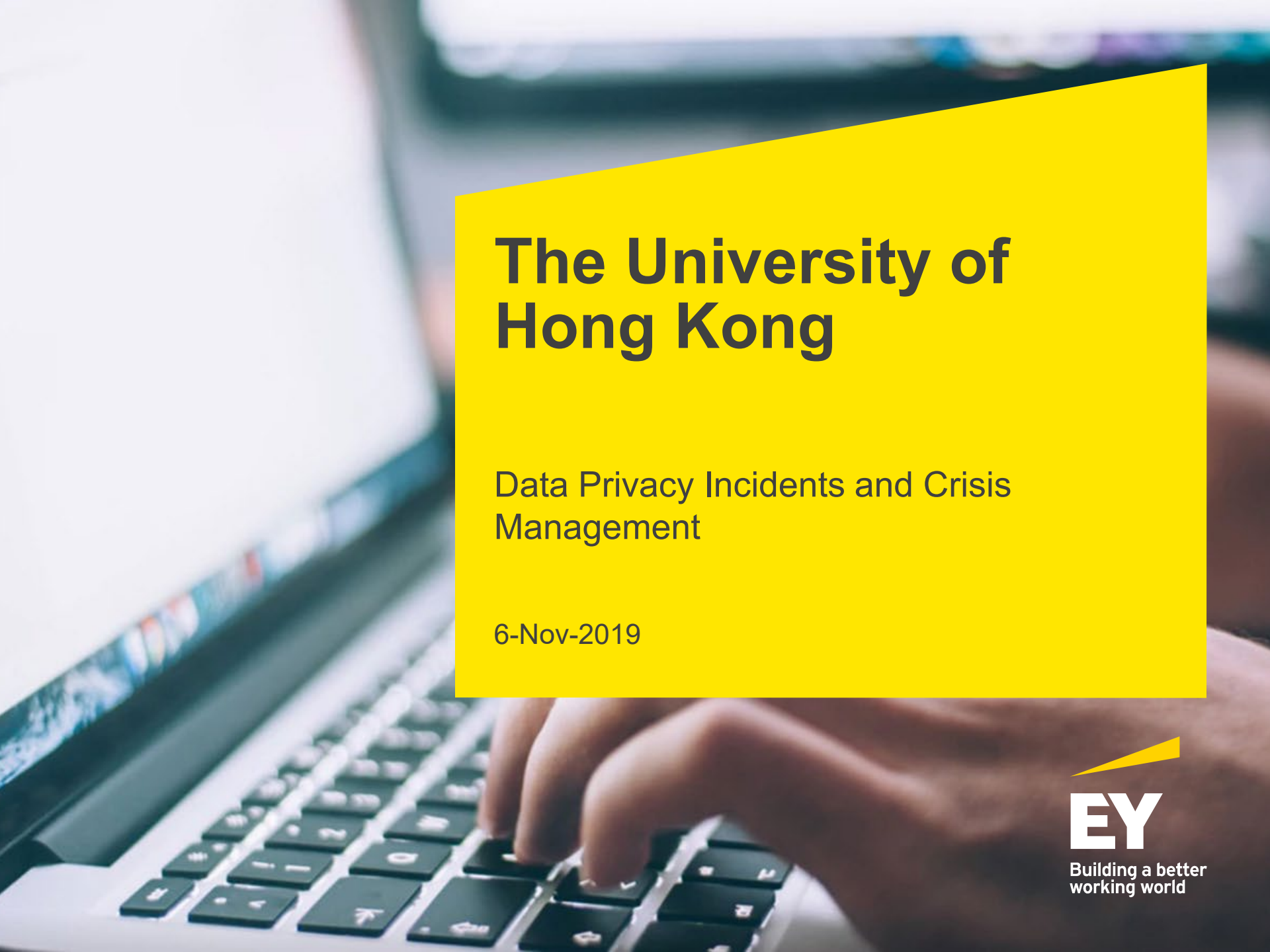


The University of Hong Kong

Data Privacy Incidents and Crisis Management

6-Nov-2019

EY
Building a better working world

Agenda

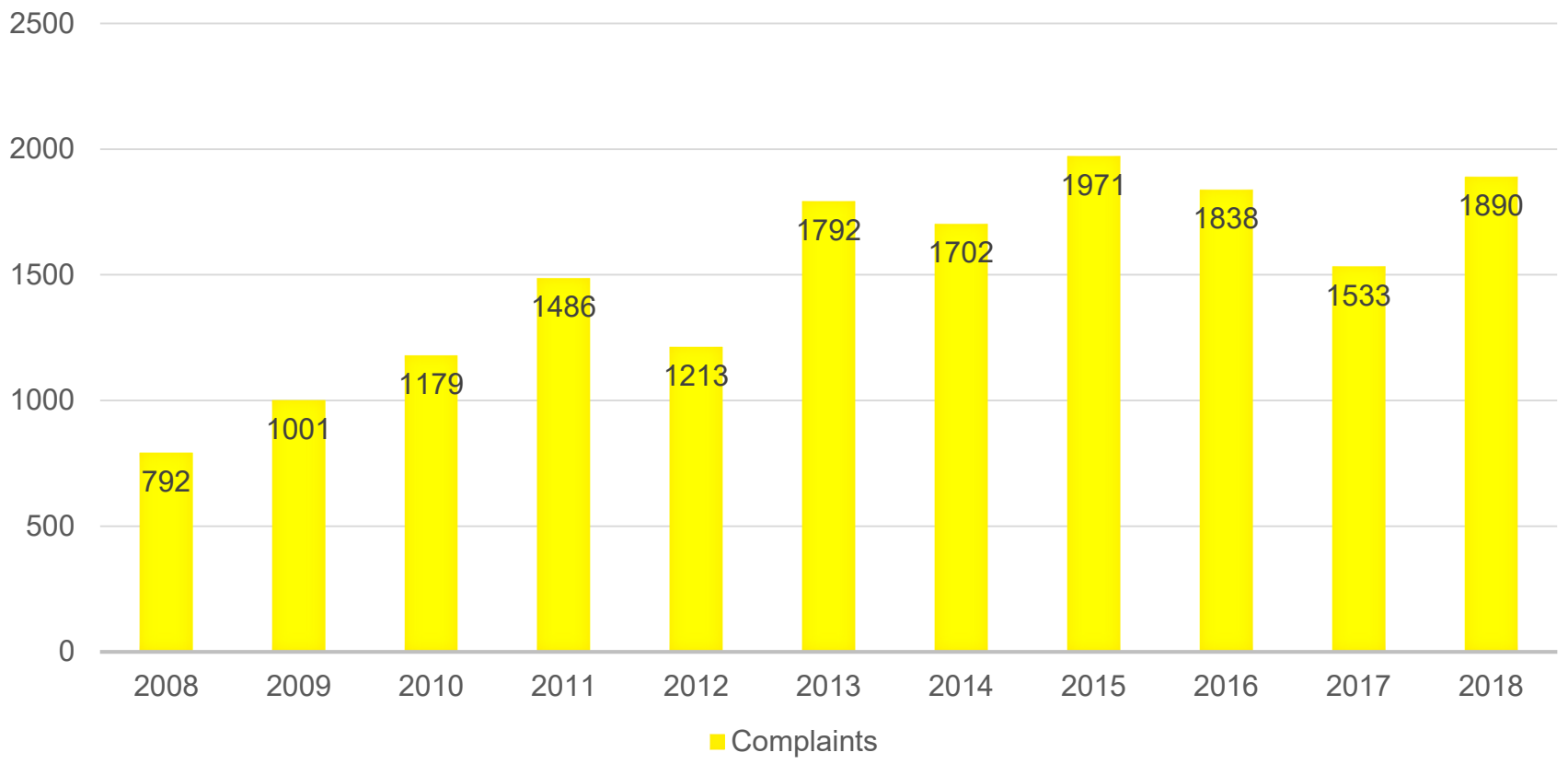
1. Personal Data (Privacy) Ordinance (Cap. 486)
2. Information Security Measures
3. Privacy Management Program and Data Inventories
4. Data Breach Incident and Crisis Management
5. The System and Practices in the University

Personal Commissioner for Personal Data (PCPD)

- An **independent statutory body** set up to oversee the enforcement of the Personal Data (Privacy) Ordinance (Cap. 486) which came into force in 1996

- To **secure the protection of individuals' privacy** with respect to personal data through:
  - Promotion
  - Monitoring
  - Supervision

Total number of complaint cases received by PCPD

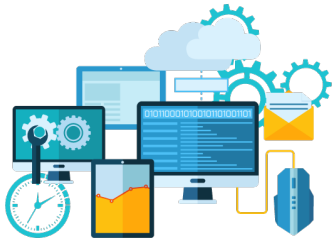


Source: https://www.pcpd.org.hk/english/complaints/statistics/statistics.html

Total number of complaint cases received by PCPD (Cont'd)

PCPD received **1890** complaints from the public in 2018

23% increase from 2017



501 complaints were related to Information & Communication Technology

270 cases were related to the leakage of personal data on the Internet

252 cases had to do with social media platforms

Source: https://www.pcpd.org.hk/english/news_events/media_statements/press_20190131.html

Personal Data (Privacy) Ordinance (Cap. 486)

Key definitions under the PDPO

- '**Personal data**' means any data -
  - (a) Relates directly or indirectly to a living individual ("**data subject**")
    - Can be used to identify that person
  - (b) Exists in a form which can be processed and accessed

e.g.

Name	**ID card number**
Phone number	**Medical record**
Address	**Employment record**

- '**Data user**' means a person who
  - Either alone or jointly or in common with other persons, controls the collection, holding, processing, usage
  - Liable as the principal for the wrongful act of its authorized data processor
- '**Data processor**' process data on behalf of the data user

Personal Data (Privacy) Ordinance (Cap. 486) (Cont'd)

Six Data Protection Principles

DPP1: Collection

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function / activity of the data user. Data collected should be adequate but not excessive.

DPP2: Accuracy & Retention

Practical steps shall be taken to ensure personal data is accurate and not kept longer than what is necessary to fulfil the purpose for which it is used.

DPP3: Data Use

Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.

Source: https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html

Personal Data (Privacy) Ordinance (Cap. 486) (Cont'd)

Six Data Protection Principles

DPP4: Data Security

A data user needs to take practicable steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use.

DPP5: Openness

A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

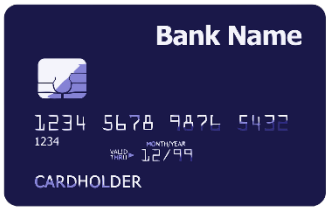
DPP6: Data Access & Correction

A data subject must be given access to his / her personal data and allowed to make corrections if it is inaccurate.

Source: https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html

What are the hackers usually looking for?

- ID card number
- Passport number
- Credit card information
- Username and password
- Birthday



What are the hackers usually looking for? (Cont'd)

- **Student PII (personally identifiable information)**
- **Cutting edge research**
- **Technology innovations**
- **Intellectual property**

What are the hackers usually looking for? (Cont'd)

- Hackers have been targeting universities in an effort **to uncover maritime technology** that is being developed for military use.
- **27 universities** were involved
- Focused on **stealing research data**
- The effort dates back to at least April 2017

Source: fortune - 5 March, 2019

Human factors

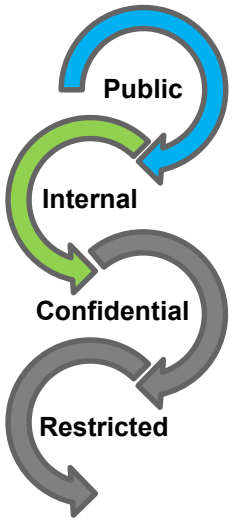
The vulnerability with the most increased risk exposure

34% of the 1,400 organizations that participated the survey see careless/ unaware employees as the biggest vulnerability.

Source: EY Global Information Security Survey 2018-19

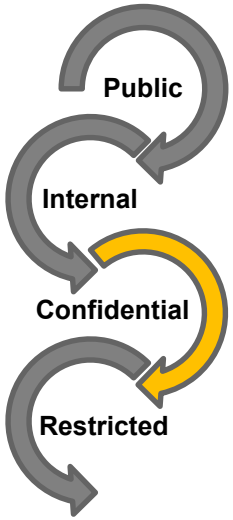
Information Security Measures

- **HKU's Data Classification Scheme**
- **Four Levels of Classification**
  - **Public**
    - Open to Public
    - No Restriction on Access
    - Present minimal perceived risk
    - i.e. HKU policies, programme information, press releases
  - **Internal**
    - Non-sensitive operational data/information
    - Disclosures are not expected to cause serious harm to HKU
    - Access may be provided to staff based on respective roles and responsibilities
    - i.e. Staff handbooks, training materials, internal procedures



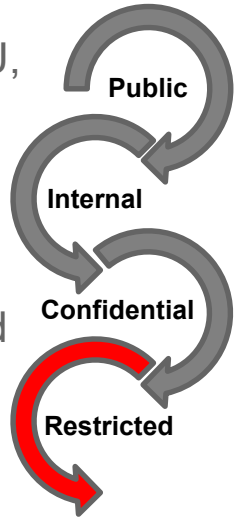
Information Security Measures (Cont'd)

- **Confidential**
  - Sensitive data/information intended for use by specific group of authorized personnel within HKU and business partners
  - Assigned on a need-to-use basis
  - Unauthorized disclosure, modification or destruction would adversely affect the business or continuity of operations
  - i.e. Student and staff personal information, unpublished research information, identifiable research subject data



Information Security Measures (Cont'd)

- **Restricted**
  - Data/information that is very sensitive in nature and restricted by HKU, the gov or any other agreements between HKU and 3rd parties
  - Critical to HKU's capacity to conduct its business
  - Used exclusively by limited numbers of predetermined and authorized individuals
  - Financial lost or damage to HKU's reputation
  - i.e. Examination papers before official release, privileged accounts' passwords, sensitive personal data (HKID, credit card information)



Information Security Measures (Cont'd)

- **Practical Tips**
  - **Work Station**
    - Complex Password
      - Minimum length of **10** characters
      - Alphanumeric
      - Non-sequential
      - Do not use default password
    - **Lock** your computer when leaving it unattended
    - Use **strong screensaver password**

Information Security Measures (Cont'd)

- **Avoid using public computer to access confidential files**
  - Public machines can be infected with **key logger malware**
  - **Disable** password saving
  - **Delete** temporary Internet files and browsing history

- **Physical Security**
  - Avoid placing workstations in **very public or private locations**
  - **Restrict access** to vulnerable workstations
  - Install **cable locks**
  - Install **privacy screen filters**
  - Loss or destruction of devices should be **reported immediately**

Information Security Measures (Cont'd)

- **Storage**
  - Encryption i.e. Azure Information Protection (AIP)
  - Organizations that collect **PII** should adopt strong encryption to protect data stored on a storage system
  - **Backup** the computer regularly
    - An encrypted disk that crashes can result in files being lost forever
  - HKU's **Data Loss Protection (DLP)** Project
    - A measure adopted by HKU for meeting **DPP4 – Data Security**
  - Always encrypt removable media
    - Store sensitive data only when it is **absolutely necessary** and **erase** the data immediately after using it

Information Security Measures (Cont'd)

- **Social Network**
  - Read the **Personal Information Collection Statement** (PICS) and **Privacy Policy Statement** (PPS)
  - Get to know **how** your personal data will be handled
  - Don't **overshare** your life details, cyberthieves might be able to use these details to access sensitive accounts
    - Consider the genuine need
    - Is the supply of my data obligatory?
  - Carefully manage your **Privacy and Security Settings**



Information Security Measures (Cont'd)

- **Mobile Security**
  - Use a **complex passcode** to lock your phone
  - Beware of what applications are **tracking your location**
    - You can disable location services in the settings app
  - **Erase** all information before repair or disposal to prevent data leakage
  - Perform **backup** regularly
    - Know what subsequent actions to be taken after data leakage
  - **Encrypt sensitive data** to provide an extra layer of protection
  - Use applications for their **intended purposes only**
    - Do not use the camera or contact app to save sensitive data

Information Security Measures (Cont'd)

- **Mobile Security**
  - Download applications from the **official app store**
    - There is a dramatic increase in the number of mobile malware
    - Remove suspicious apps
  - Connect to **trusted Wi-Fi** spots only
    - Prevent Man-in-the-middle attack, eavesdropping
  - **Update** the OS regularly
    - Install the latest **security patch**

- Be sure to visit ITS booth at Chi Wah Learning Common for more mobile security tips!

Privacy Management Program (PMP) and Data Inventories

- PCPD has advocated that **identified sectors (banking, insurance, telecommunications and insurance)** should **develop and maintain a PMP** (for the promotion of accountability)

- To ensure that **appropriate policies and procedures are in place to promote good privacy practices** in the following areas (Feb 2013): Organization commitment, program controls, monitoring and annual review of program control effectiveness, and assessing and updating program controls.

- **39 companies and organizations had pledged** in Feb 2014 to implement the PMP.

Source: https://www.pcpd.org.hk/english/news_events/whatison/files/PCPD_AmCham_9Dec2015.pdf

Privacy Management Program (PMP) and Data Inventories (Cont'd)

- Organization commitment
- Programme controls
  - Personal data inventory
  - Internal policies on personal data handling
  - Risk assessment tools
  - Training, education and promotion
  - Handling of data breach incident
  - Data processor management
  - Communication
- Ongoing Assessment and revision
  - Development of an oversight and review plan
  - Assessment and revision of programme controls

Privacy Management Program (PMP) and Data Inventories (Cont'd)

- "An organization should know what kinds of personal data it holds (for example, personal data of employees, personal data of customers, etc.), how the personal data is being used – and whether the organization really needs it at all"
- "Every component of an accountable, effective **privacy management programme** begins with this assessment." – Privacy Management Programme : A Best Practice Guide

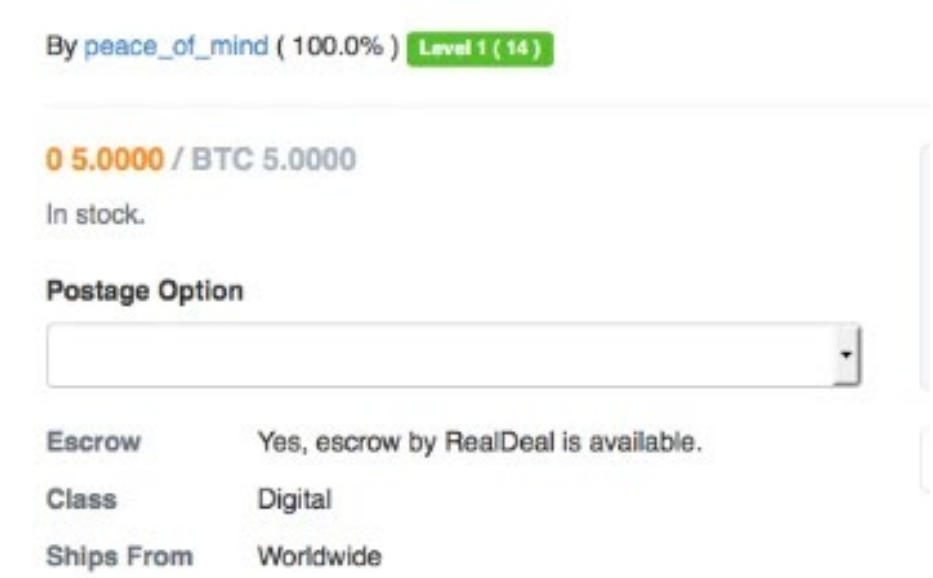
Purpose	Sub Process	Dataset Index	Dataset Name	Data Form	Location	Types of Personal Data	Data	Data Purpose	Retention	Security	Source from	Means (in)	Means (in) Retention	Transfer to	Means (out)	Means (out) Retention
Staff Administration	Security Guard Qualifications		CVs	Electronic	Security Branch responsible person Inbox/ Outbox	Personal Details	Name of Guards	Verification of person	No Retention	Email restriction	Contractor Company	Email	N/A	N/A	N/A	N/A
						Personal Details	Full HKID no	Verification of person	No Retention							
						Personal Details	Date of Birth	Staff Administration	No Retention							
						Personal Details	Age	Staff Administration	No Retention							
						Personal Details	Residential Distri	Staff Administration	No Retention							
			internal qualifcaitan list	Electronic	Security Branch local drive	Personal Details	Name of Guards	Verification of person	Permantely	Local drive	Individualr	Interview	N/A	N/A	N/A	No Retention Policy
						Personal Details	First four digit of HKID No.	Verification of person	Permantely							
						Personal Details	Date of Birth	Staff Administration	Permantely							
						Personal Details	Age	Staff Administration	Permantely							
						Personal Details	Residential Distri	Staff Administration	Permantely							
			external qualification list	Electroni	Security Branch local drive	Personal Details	Name of Guards	Verification of person	No Retention	Local Drive	Internal qualifcaitan list	N/A	No Retention Policy	Central Room/ G4S	Email	No Retention Policy
						Personal Details	DOB	Staff Administration	No Retention							
						Personal Details	Age	Staff Administration	No Retention							
						Personal Details	Residential Distri	Staff Administration	No Retention							
			external qualification list	Electroni	Central Room Inbox	Personal Details	Name of Guards	Verification of person	No Retention Defined	Email Restriction	Security Branch	Email	No Retention Policy	N/A	N/A	N/A
						Personal Details	DOB	Staff Administration	No Retention							
						Personal Details	Age	Staff Administration	No Retention							
						Personal Details	Residential Distri	Staff Administration	No Retention							

Privacy Management Program (PMP) and Data Inventories (Cont'd)

Column	Meaning	Example
Data Purpose	The purpose of collecting or retaining the data field	Supporting for account opening / tax reporting
Retention Period	How long the dataset is retained for	7 years / 3 years after the termination of account
Security	How the dataset is secured at the location	Locked cabinet / encryption / access control / masking / password protection
Source From	Where the dataset is sourced from	Customer / another department / another company
Means (in)	How the dataset is sourced in	Collected online / email / by hand / downloaded from share drive
Means (in) Retention Period	How long the dataset is retained for in the source-in location e.g. mailbox	7 years / 3 years after the termination of account
Transfer to	Where the dataset is transferred to	Another department / another company / system
Means (out)	How the dataset is transferred out	Email / by hand / fax / uploaded to system
Means (out) Retention Period	How long the dataset is retained for in the source-out location	7 years / 3 years after the termination of account
Means (out) Security	How the dataset is secured at the source-out location	Encryption / access control / password protection

Data Breach Incidents

- **Social networking data breach**
  - Back in 2012, account information (Email address & password) of 117 million users have been hacked
  - 4 years later, the massive batch of login credentials have been posted on the black market



Source: Vice – 18 May 2016

Data Breach Incidents (Cont'd)

- **Major airline company's data breach incident in 2018**
  - Personal data of **9.4 million** passengers was leaked [1]
  - Names, nationalities, telephone numbers, emails, physical addresses, ID card numbers etc. [1]
  - **860,000** passport numbers and **245,000** HKID numbers were accessed without authorization [2]

Source: [1] Forbes – 6 Jun 2019 ; [2] SCMP1 – 24 Oct 2018

Data Breach Incidents (Cont'd)

- Suspicious activity was detected in **March**
  - Started an investigation with the help of a cybersecurity firm to strengthen the information system security measures [1]
- Unauthorized access to the data was confirmed in **May**
  - The combination of data accessed varied for each affected passenger [1]
- The incident was not disclosed until **October** [1]
- Another airline company has been handed a record **£183 million** fine for a similar incident [2]

Source: [1] SCMP1 – 24 Oct 2018 ; [2] SCMP – 9 Jul 2019

Data Breach Incidents (Cont'd)

- **The Privacy Commissioner's Enforcement Notice:**
  - Engage an **independent data security expert** to overhaul the systems containing personal data and conduct reviews of the airline's network security
  - Implement effective **multi-factor authentication** to all remote users for accessing its IT system
  - Conduct effective **vulnerability scans** at server and application levels
  - Devise a **clear data retention policy** to specify the retention periods of passengers' data
  - Completely **obliterate all unnecessary HKID Card numbers** collected from the membership programme

Source: PCPD

The EU General Data Protection Regulation (GDPR) (Cont'd)

Right to

bility

Breach No

ection
ers

- Mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals"
- Must be done within **72 hours**
- Data processors are required to notify their customers & data controllers without undue delay

The EU General Data Protection Regulation (GDPR) (Cont'd)

- Organizations in breach of GDPR can be fined up to:
  - **4%** of annual global turnover
  - €20 million

- Maximum fine that can be imposed for the most serious infringements
  - Not having sufficient customer consent to process data
  - Violating the core of Privacy by Design principles

- The rules apply to **both** data controllers and processors – meaning "clouds" are not exempt from GDPR enforcement

Crisis Management

Self-assessment

- Would you be able to identify sensitive information and perform simple data classification?
- Are you working with your IT team to ensure that you have appropriate security controls in place?
- Do you have a response team in place including senior management, key personnel and IT?

Crisis Management (Cont'd)

Containment

Breach notification

Investigation

Remediation

Crisis Management (Cont'd)

- **C.A.R.E**
  - **C**ontaining the data breach to prevent further compromise of personal data
  - **A**ssessing the data breach by gathering the facts and evaluating the risks, including the harm to affected individuals. Where assessed to be necessary, continuing efforts should be made to prevent further harm even as the organization proceeds to implement full remedial action.
  - **R**eporting the data breach to all affected individuals and the PCPD, if necessary.
  - **E**valuating the organization's response to the data breach incident and consider the actions which can be taken to prevent future data breaches. Remediation efforts may continue to take place at this stage.

Crisis Management (Cont'd)

- **C.A.R.E**
  - An organization should act swiftly as soon as it is aware of a data breach.
  - An assigned individual should activate the response team to reduce the potential impact of the data breach.
  - An initial assessment should be conducted to determine the severity of the data breach.

    - **Cause of the data breach and whether it is still ongoing**
    - **Number of affected individuals**
    - **Types of personal data involved**
    - **The affected systems and services**
    - **Whether external assistance is required to contain the breach**

Crisis Management (Cont'd)

- **C.A.R.E**
  - The assessment allows organizations to decide on the immediate actions to be taken.

    - **Isolate the compromised system from the Internet or network**
    - **Prevent further unauthorized access to the system. Reset passwords and change the access rights to the compromised system, where applicable.**
    - **Stop the identified practices that led to the data breach**
    - **Establish whether the lost data can be recovered and steps that can be taken to minimize any harm or impact caused by the data breach**

  - Evidence of the data breach and post-breach response should be kept and recorded in an Incident Log respectively to facilitate follow-up investigations.

Crisis Management (Cont'd)

- **C.A.R.E**
  - Upon the containment of the data breach, an in-depth assessment should be conducted to identify and limit the impact and damage.
    - **Context of the data breach**
    - **Ease of identifying individuals from the compromised data**
    - **Circumstances of the data breach**
  - The in-depth assessment should allow organizations to conclude whether the data breach is likely to result in significant impact to the affected individuals.
  - Organizations can take steps to reduce any potential harm to the affected individuals.

Crisis Management (Cont'd)

- **C.A.R.E**
  - Organizations should have in place appropriate processes to notify the affected individuals and the PCPD, if necessary.
    - **Who needs to be notified?**
    - **How should the affected individuals be notified?**
    - **What details should be included in the notification?**
    - **When should the notification be done?**
  - If a data user decides to report a data breach to the Privacy Commissioner, the data user may complete a Data Breach Notification Form and submit the completed form online, by fax, in person or by post.

Crisis Management (Cont'd)

- **C.A.R.E**
  - The organization should review and learn from the data breach incident to improve its personal data handling practices and prevent the reoccurrence of similar incidents.
    - **Data breach management plan and response**
    - **Existing measures and processes**
    - **Roles of external parties**
  - Regular trainings should be provided to all employees so as to raise their overall security awareness.

Crisis Management (Cont'd)

Hope for the best, prepare for the worst

The System and Practices in the University

- Information Security and Data Management Policy: https://isdm.hku.hk/
- The Privacy Policy Statement (revised version 2015): http://www.hku.hk/privacy_policy/
- Code of Practice (revised version 2019): https://intraweb.hku.hk/reserved_1/gsabc/pdpo_cop.pdf (portable storage devices, incident handling / reporting and other guidelines)

The System and Practices in the University

- Data Collection Statement
- Statutory Data Access / Correction Request Process
- Central Compliance Team (compliance/monitoring)
- University Data Protection Officer and Personal Data Protection Coordinators
- Information Technology Services (advice / security measures / guidelines / training information): http://www.its.hku.hk/services/training/infosec/personal-data-protection

The University of Hong Kong

The System and Practices in the University

The Public Expectation

Awareness and Education

GOOD PRACTICE

The University of Hong Kong

Thank you!

Appendix

https://www.pcpd.org.hk/english/complaints/statistics/statistics.html

https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html

https://www.scmp.com/news/hong-kong/transport/article/2170076/personal-data-some-94-million-passengers-cathay-pacific-and

https://www.slideshare.net/BradfordBach/data-breach-presentation-55919814

https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/PCPD_Investigation_Report_R17-6429_Eng.pdf

https://www.pcpd.org.hk/english/news_events/media_statements/press_20190606.html

https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Managing-Data-Breaches-2-0.pdf

https://eugdpr.org/the-regulation/

https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

https://money.cnn.com/2016/05/19/technology/linkedin-hack/

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

APAC no.
ED MMYY

ey.com/china