



Secure Your Business Against Security Threats



Protecting Data Privacy and Preventing Data Leakage



*Henry Chang, IT Advisor
Office of the Privacy Commissioner for Personal Data, Hong Kong
11 April 2013*

1



Personal Data Definition

Any data:

- 1. relating directly or indirectly to a living individual;**
- 2. from which it is practicable for the identity of the individual to be directly or indirectly ascertained;
and**
- 3. In a form in which access to or processing of the data is practicable.**



The Six Data Protection Principles

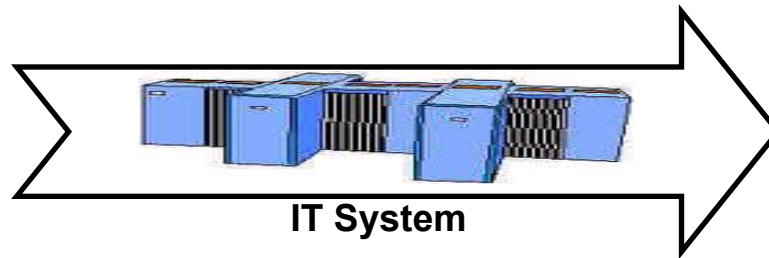
Personal Data Flow

Collection



DPP 1 – Collection

Storage, Use or Processing



DPP 3 – Use

Retention/
Erasure



DPP 2 – Accuracy
and retention

DPP 4 – Security (IT and physical)
DPP 5 – Transparency
DPP 6 – Rights of access and correction

3



Top-down Approach

access-administration access-authorisation access-control
access-recertification **accountability** assessment audit
audit-trail availability backup-tapes bcpr certification
confidentiality data-breach-management **data-**
classification data-loss-prevention decommissioned-systems development
-environment disposal-policy **documentation** encryption
erasure-policy firewall **governance** hr-policy incident-management
information-owner **integrity** iso-27000 mobile-policy password
-control penetration-test pia portable-storage-devices-policy privacy-by-
design privileged-access retention-policy review security-policy
segregation-of-duties segregation-of-environment service-provider
shared-access testing-environment training-and-awareness



Data Breach through websites

‘Low tech’ causes:

- 1. Unaware of the legal requirements to protect personal data**
- 2. Use website as temporary storage (obscurity is no security!)**
- 3. Inappropriate reliance on functions of website builders**
- 4. No housekeeping after system maintenance**



Data Breach through websites

‘Low tech’ prevention and cure :

- 1. Having proper policies and guidelines**
- 2. Using search engine ‘hacks’ as a detection tool**
- 3. Knowing how to remove cached copies in search engines**
- 4. Knowing how your website/website builder works**



Data Breach through websites

‘High tech’ causes:

- 1. Not applying security patches (have you patched your Java?)**
- 2. Inappropriate password reset processes**
- 3. Weak password complexity and controls**
- 4. Weak access control mechanism**
- 5. ‘Predicable’ URLs (web addresses)**



Data Breach through websites

‘High tech’ prevention and cure :

- 1. Formal security patch management**
- 2. Vulnerability scanning/testing**
- 3. Proper password complexity and reset controls**
- 4. Encrypting data at rest and data in motion**
- 5. Employing staff or contractors with security knowledge**



Physical Data Breach

Causes:

1. Disposal of various types of storage media
2. Use of portable storage devices



Physical Data Breach

Prevention and cure :

1. Having formal disposal policy
2. Having proper risk assessment and portable storage device policy



Helps available in PCPD

- **Guidance for Data User on the Collection and Use of Personal Data through the Internet***
- **Guidance on the Use of Portable Storage Devices***
- **Guidance on Personal Data Erasure and Anonymisation***
- **Seminar/workshops held in PCPD****

*All available under http://www.pcpd.org.hk/english/publications/guid_note.html

** <http://www.pcpd.org.hk/english/activities/promotion.html>



Secure Your Business Against Security Threats



Thank You

