Managing IT Risks

Chong Yoke Sin
CEO, IHIS

Agenda

1. **IT risk definition and risk matrix**
2. **Types of IT risks**
3. **PDPA**

1 Survey Results from Singhealth

- 56.9% indicated managing risk is top concern
- 78.9% indicated that they were briefed on need to manage IT risks on the job
- 53.2% were not aware and 34.9% were unsure of what data/information needed to be protected and legal implications of use and disclosure of personal data of patients/individuals

Industry Trends

The changing face of information security 2006-2012

Key trends in information security 2006-2012

2006-2007

Before 2006 information security was a component of mitigating financial risk and meeting new compliance requirements (e.g. SOX 404)

After 2006, information security needed to:

- Protect the organization more broadly in a globalized world
- Demonstrate a clear return on investment, requiring an alignment of risk and performance

2008-2009

Against a background of global financial crisis and a changing competitive landscape, information security matured beyond compliance.

In an environment of escalating threats:

- Protecting brand and reputation was primary driver
- Leveraging technology to increase security was a focus
- Organizations also needed to concentrate on reshaping, restructuring and reinventing to keep up with new requirements and cost pressures.

2010-2011

Global economy still in recovery with sustained cost pressures and scarce resources.

Companies realized:

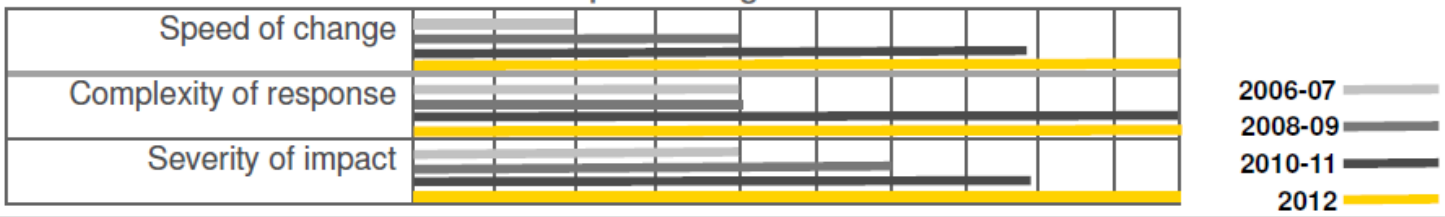
- With globalization, data is everywhere
- Traditional boundaries were vanishing, with employees sending data over the internet or carrying it on mobile devices
- Data processing moved into the cloud, requiring information security function to rethink its approach to securing information

2012

Velocity and complexity of change accelerates:

- Virtualization, cloud computing, social media, mobile and other new technologies open the door to internal and external threats.
- Emerging markets, continuing economic volatility, offshoring and increasing regulatory requirements add complexity.
- Organizations unable to keep pace with changes, create an information security gap.

Impact on organizations



Fighting to close the gap: Ernst& Young's 2012 Global Information Security Survey

ERNST & YOUNG
Quality In Everything We Do

Usual Risk Terms

- Annualized Loss Expectancy –
  - The Cost of loss due to a Risk over a year
- Threat – A Potentially negative occurence
- Vulnerability – A Weakness in a System
- Risk – A Matched Threat and Vulnerability
- Safeguard – A Measure taken to Reduce Risk
- Total Cost of Ownership – The Cost of a Safequard
- Return of Investment – Money Saved by deploying a Safeguard

Risk = Threat x Vulnerability x Impact

Risk Analysis Matrix

Qualitative Risk Analysis Matrix - Level of Risk *

Likelihood	Consequences				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
A (almost certain)	M	H	H	E	E
B (likely)	M	M	H	H	E
C (possible)	L	M	M	H	E
D (unlikely)	L	M	M	M	H
E (rare)	L	L	M	M	M

* Level of risk:

(E) Extreme risk - detailed action/plan required

(H) High risk - needs senior management attention

(M) Moderate risk - specify management responsibility

(L) Low risk - manage by routine procedures

Please note that this template may require revision, dependant upon the analysis of your Agency's risk exposures.

Risk Choice

- Accept the Risk
- Mitigate the Risk
- Transfer the Risk
- Risk Avoidance

Preserving Data Confidentiality

Confidentiality is a term that indicates preserving the privacy of the individuals who receive care (Goldman&Mulligan,1996). This means that all information related to the patient will be kept in strict confidence for use only by the team of healthcare providers. This includes information gained verbally or from the individuals medical records. All information is considered confidential when it pertains to medical care.

IT risk group

- CISO in charge of IT risk policy and management
- Compliance group to ensure conformance
- Security policy group reports to CIO
- Prepares for audits – both internal and external
- Conduct of training and change management

Obligations of IT systems for Risk management

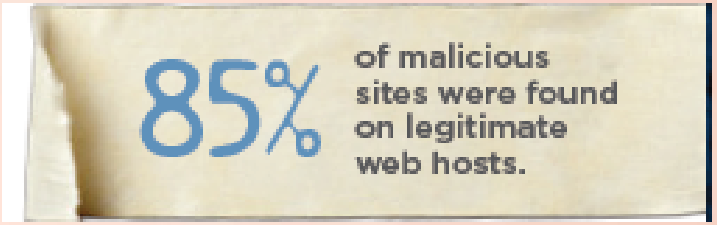
- Execute the consent choice of Patient within the system
- Ensure Accuracy, Retention and Protection of Data already captured
- Ensure Systems Availability and availability of captured data

Obligations of Users of IT systems

- Capture Patient's consent re medical record's inclusion(default) or exclusion
- Do not share patient's medical records outside permitted boundaries of medical care
- Do not leak patient's records to other non-permitted parties

Security Threats

- **Web Threats**
- **Social Media Threats**
- **Mobile Threats**
- **Email Threats**
- **Malware Behavior**
- **Data Theft/Data Loss**

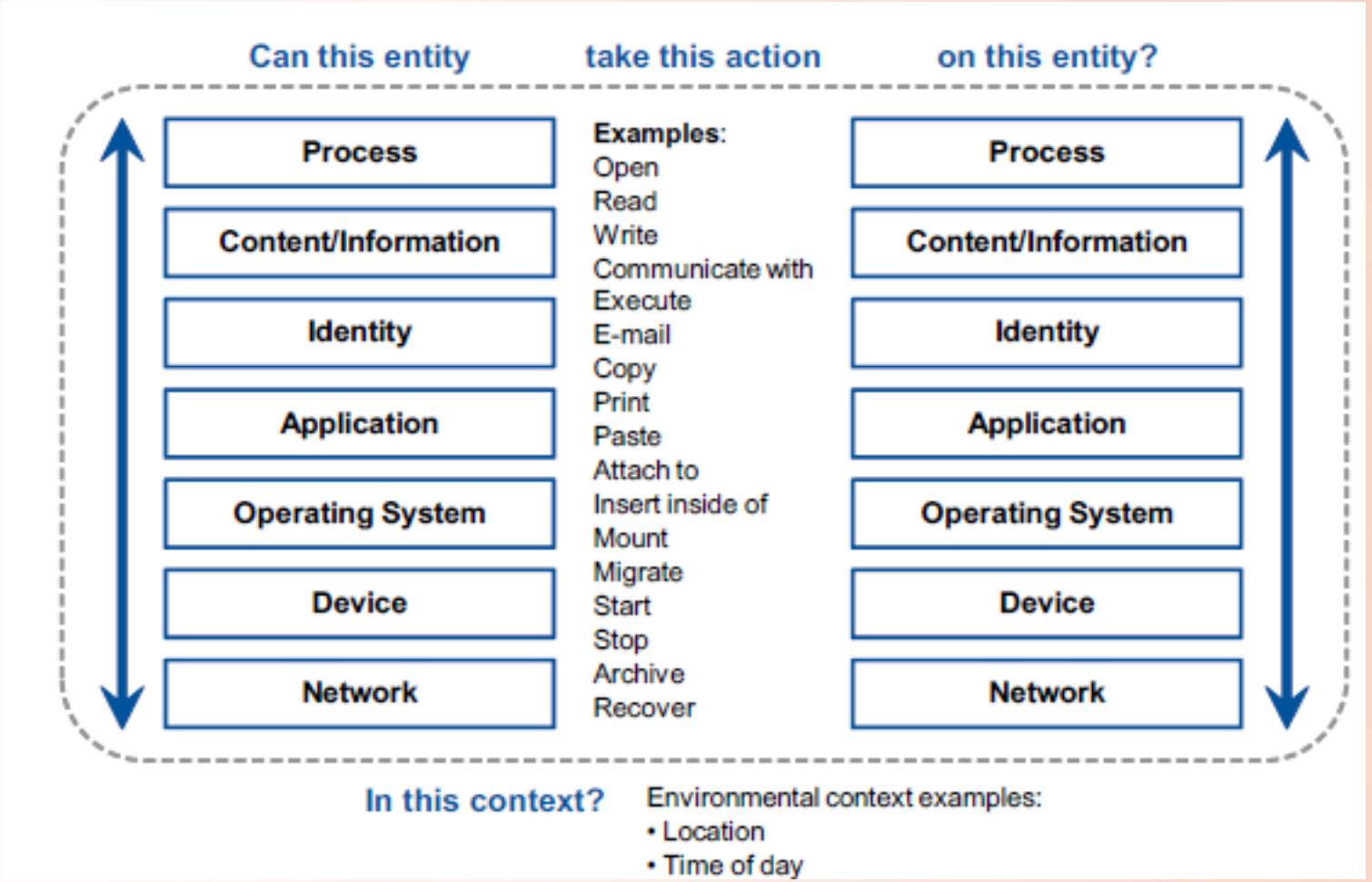


Websense 2013 Threat Report

Information security coverage

- Endpoint security and mobility
- Network and data center security
- Application and software security
- Data security
- Cloud security
- Monitoring trends
- Vulnerability management

Information Security Decisions among entities



Examples of Information security Decisions

Context Layer	Example Categories at This Layer	Examples of Contextual Information at This Layer
Environmental	Local environment Macroenvironment	Location Prior location Proximity Time of day, month, year Time elapsed since last action Temperature Ambient lighting
Community	Friends Family Social networks	Relationships Patterns of uptake Presence Links Tagging
Process	Customer facing Revenue producing	Importance of the process Impact on revenue if down SLA requirements Current users of the process
Content	Files Databases Executable content E-mail Input	Sensitivity of content Trust of the content Reputation of executable code Reputation of the e-mail Known vulnerabilities Input from the collective
Identity	Organization User Group	Reputation of the user Strength of authentication Current role Team membership Clearance level Transaction amount limit Credit rating
Application	Application Service Transaction APIs Uniform resource identifier (URI)/URL	Reputation of the application Reputation of the URL Sensitivity of the transaction Amount of the transaction Historical patterns of behavior Patch level Known vulnerabilities SLA requirements

Examples of Information security Decisions

Context Layer	Example Categories at This Layer	Examples of Contextual Information at This Layer
Operating System	Processes Threads System calls Device drivers Virtualization platform	Historical patterns of behavior "Health" of the OS Patch level Known vulnerabilities Root of trust measurements
Device	Device type Virtual machine or physical IP Address	Reputation of the IP address Device reputation "Health" of the device Managed/unmanaged Enterprise owned? Storage encrypted? Strength of encryption? Accelerometer data
Network	Packets Connection types Port/protocol	Traffic encrypted? Strength of encryption? Historical patterns of behavior Known vulnerabilities

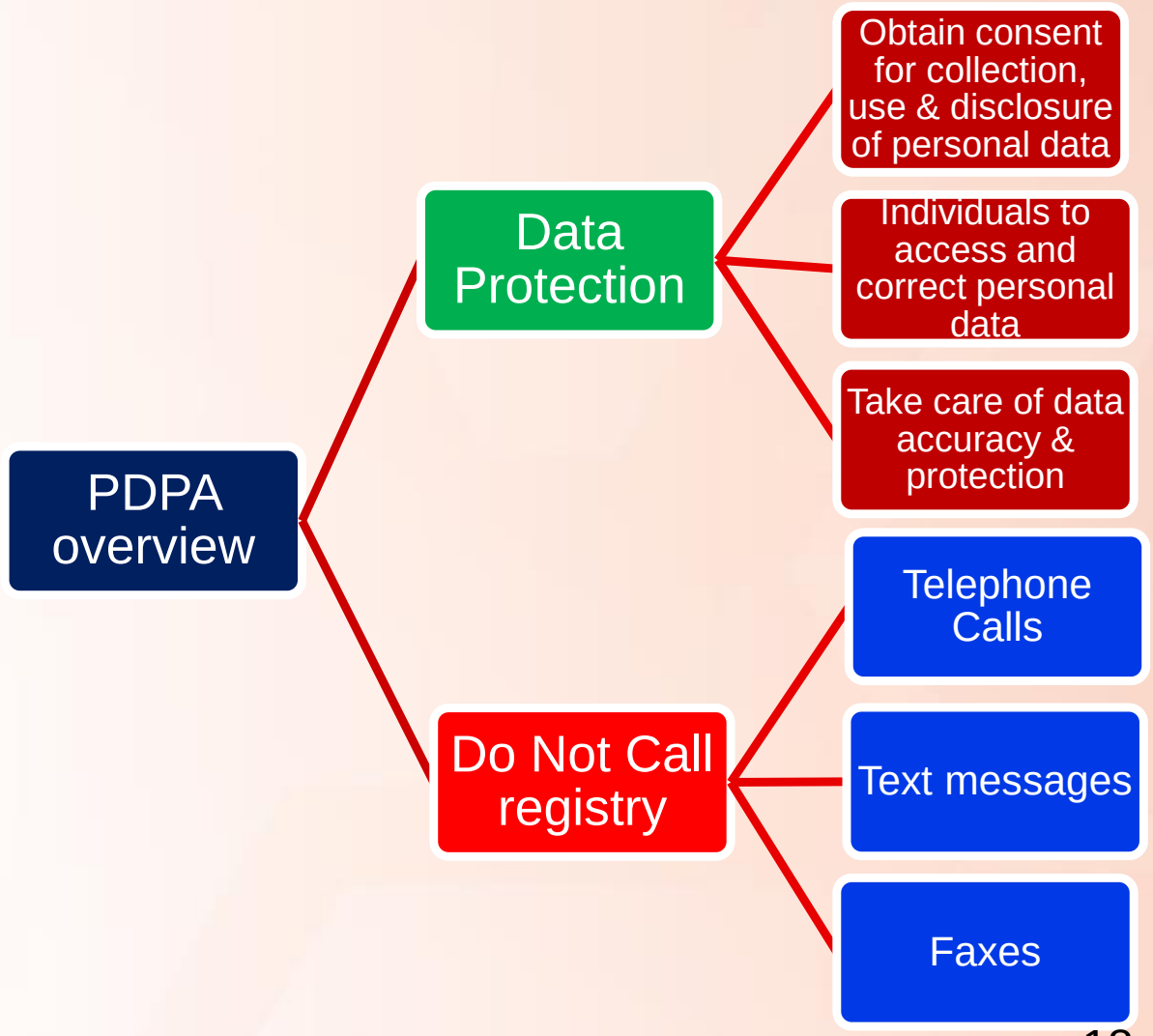
Source: Gartner (May 2010)

Purpose of PDPA, effective 1st July 2014

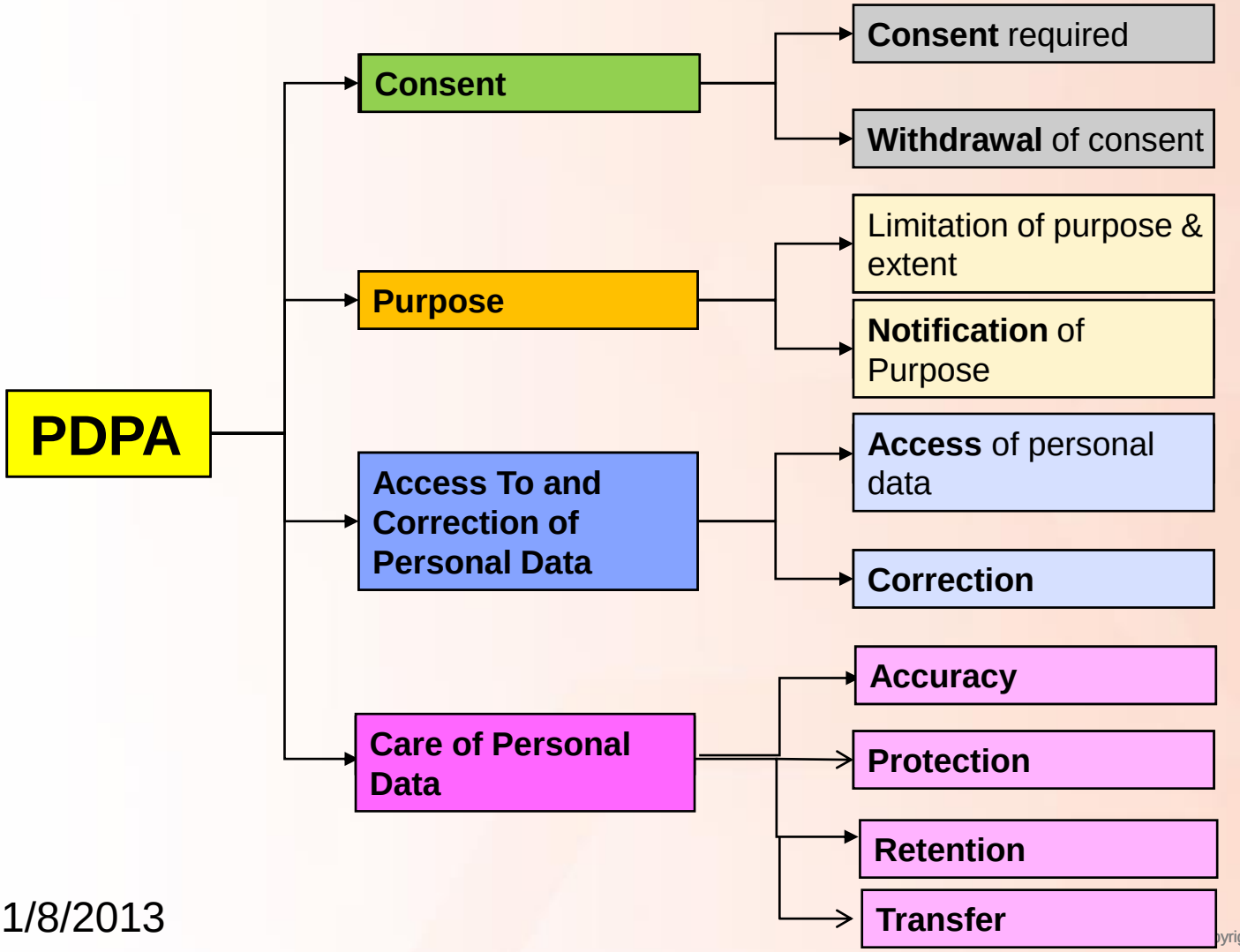
The purpose of this Act is to **govern the collection, use and disclosure of personal data** by organisations in a manner that recognises both the right of individuals to **protect their personal data** and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

PDPA recognises :

a) the right of individuals to protect their personal data;
b) the need of organisations to collect, use and disclose personal data for stated reasonable purposes.



PDPA 2012 comes into effect in July 2014.



To comply with PDPA :

- Appoint Data Protection Officer
- Implement data protection policy & procedure
- Staff communication
- Compliance audit
- Complaint Handling

1/8/2013

Summary

- Mitigate IT Risks with awareness and education
- Monitor and refine policies and governance

THANK YOU

Chong Yoke Sin

Chong.yoke.sin@ihis.com.sg

Integrated Health Information Systems
Tel: (65) 6594 1800 Fax: (65) 6594 1900