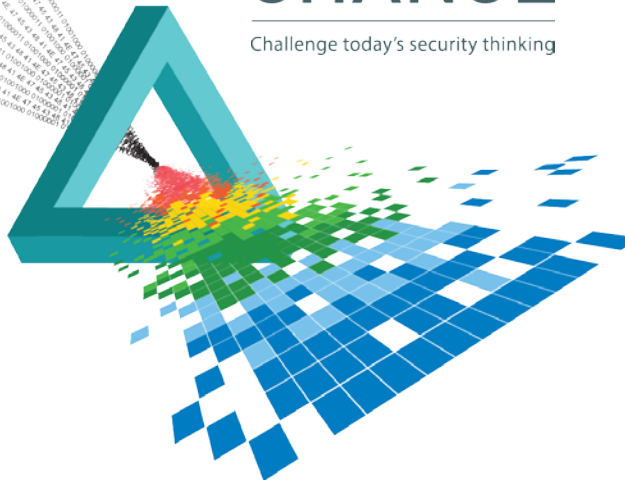
RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

CHANGE
Challenge today's security thinking



SESSION ID: CDS-F04

Getting Serious about Privacy and Cyber Security in Asia Pacific

Scott Thiel
Partner
DLA Piper
@DLA_Piper

Peter Jones
Partner
DLA Piper
@DLA_Piper

Agenda

- Current threat environment
- Regulatory frameworks of countries in the Asia Pacific region
- Key challenges and practical issues for multinational business
- Asia Pacfic enforcement conclusions

Current Threat Environment

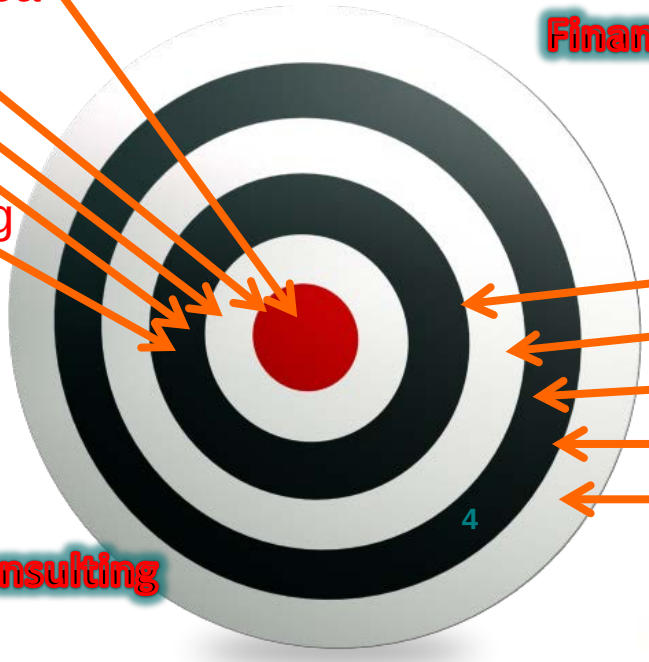
- High profile examples of data breaches
  - **2011 - *Sony's PlayStation Network attack***
  - **2013 - *Breach of information held by Adobe and theft of Acrobat source code***

- Data security is a concern in many countries in the Asia-Pacific region, e.g.:
  - **2013 - *Online accounts of staff and students of the University of Hong Kong have been attacked by hackers***
  - **2014 - *PayPal flaw discovered by tests***
  - **2014 - *BIGGEST-ever breach of private security in South Korea***

Current Threat Environment

- Asia Pacific as a region is **2 times more likely** to be targeted!
- According to the FireEye Blog, the **TOP 10** most targeted countries in Asia in 2013 are:

1. South Korea
2. Japan
3. Taiwan
4. Thailand
5. Hong Kong



Finance/ Banking

6. The Philippines
7. India
8. Australia
9. Pakistan
10. Singapore

Government

Consulting

Current Threat Environment

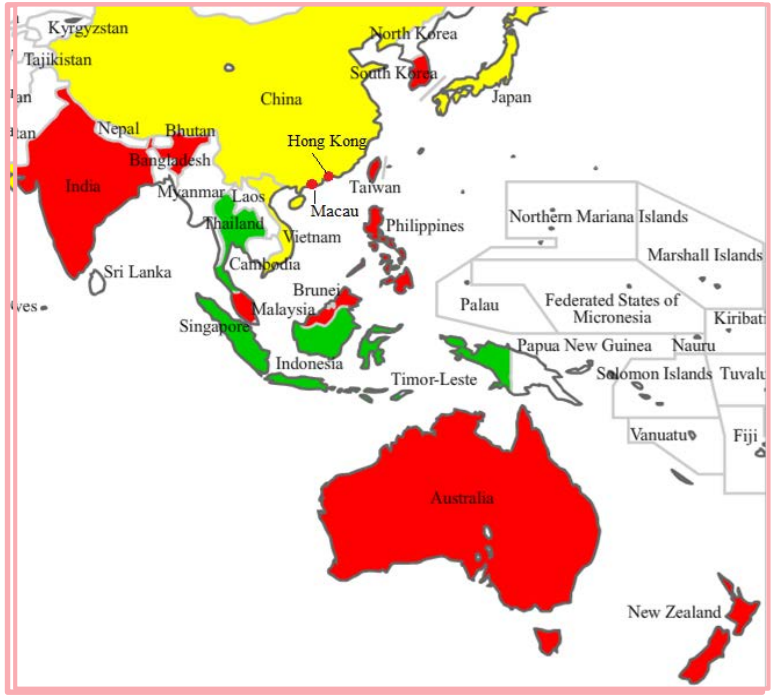
- Data Breaches exposed weak defences of organisations in the Asia Pacific region
- Data Breaches may have a Global Impact
  - Companies, banks, governments, etc. are all trying to bolster data security
- Asia Pacific countries are fighting back!

Current Threat Environment - Strategic Importance

- Diverse and evolving legal and regulatory landscape
- Exponential growth of information
- Growing protection challenge
- Corporate requirements and privacy collide
- Data and information breaches/disputes
  - High cost of mistakes

Asian Data Privacy Regimes At-A-Glance

Before (2011) **At 2014**



DLA PIPER

Asian Data Privacy Regimes At-A-Glance

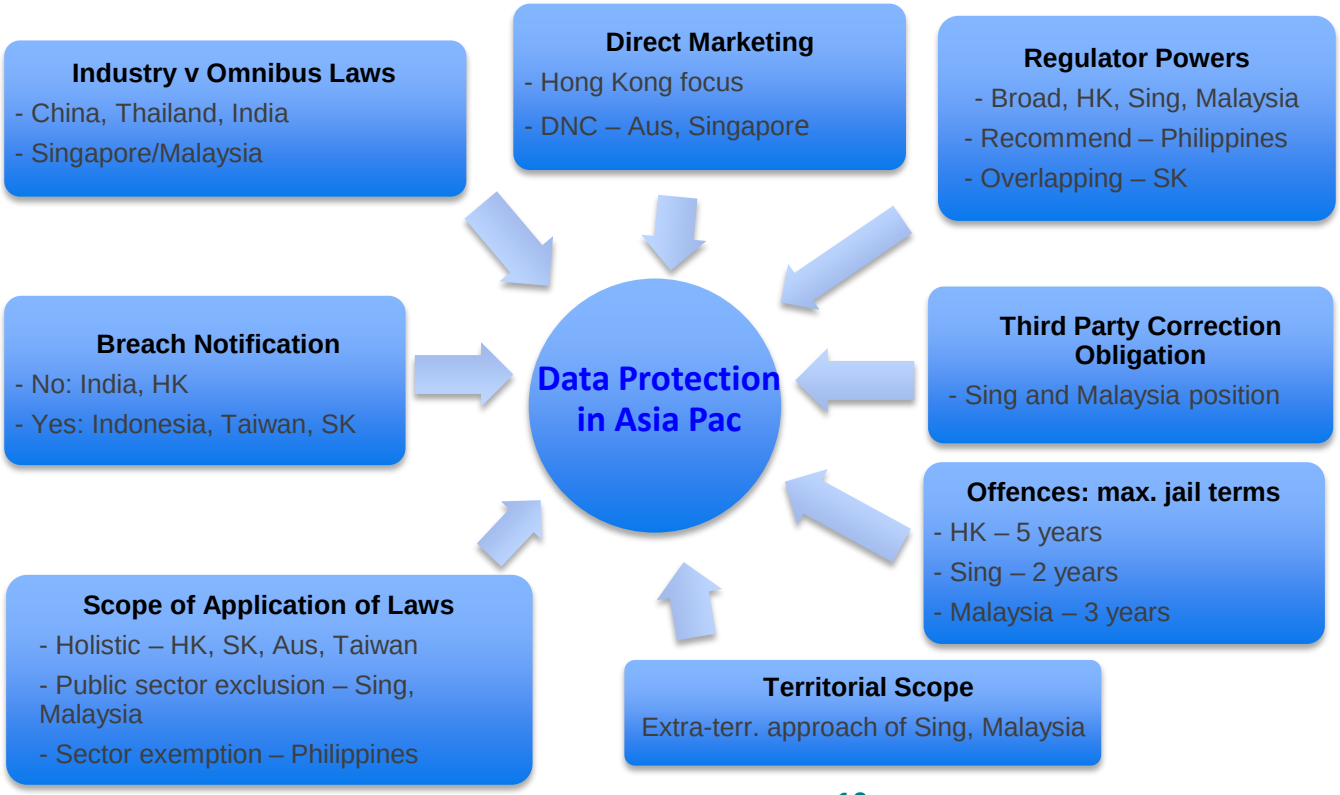
Asia-Pac region – a rapidly maturing DP landscape

- New laws – Malaysia, Philippines, Singapore
- Recent laws – South Korea
- Updates - Australia, Hong Kong, Taiwan, Vietnam
- Update scheduled - Indonesia
- Major changes expected – PRC, India (Justice (Shah's report*)

Data Protection: Regional temp

Jurisdiction	DP Law?	Collection Restrictions	Transfer Restrictions	Criminal / Admin Liability	Fines / Prison?	Overall DP Risk Level
Australia						
China						
Hong Kong						
Indonesia						
Korea						
New Zealand						
Philippines						
Singapore						
Taiwan						
Thailand						
Vietnam						

But the devil is in the detail



A Brief Survey: China

- Current Legal Regime: Combination of various non-DP specific laws (criminal law, civil law, tort law, constitution) with limited legal effect
- Major Recent Developments:
  - Decision of the Standing Committee of the National People's Congress for Enhancing the protection of Internet based Information: –
    - Applies to "Internet service providers and other enterprises or public institutions"
    - Enshrines principle of legality, legitimacy and necessity
    - Need to specify the purpose, manner and extent information collection
    - Obtain the consent of the target persons
    - Take technical and any other necessary measures to protect the security of personal information
    - Data correction obligations
    - Meaningful sanctions

A Brief Survey: China

- Major Recent Developments:
  - Information Security Technology - Guide for Personal Information Protection within Public and Commercial Information Systems published on 1 February 2013
    - Issued by the MIIT
    - Applies to private sector use of "information Systems"
    - Not Legally Binding however……
    - Prohibits extraterritorial transfer without express consent
    - Imposes security obligations
  - Chinese Supreme People's Court has recently released the Provisions of the Supreme People's Court on Issues Concerning the Application of Law in Hearing Civil Dispute Cases Involving the Infringement of Personal Rights and Interests through the Internet

A Brief Survey: Hong Kong

Regime	*Personal Data (Privacy) Ordinance ("PDPO")*	
Registration	O	• No requirement
Collection & Processing	O	• Notification + Consent (for new purpose) of Data Subject • New Consent requirements for direct marketing commence 1 April 2013
Transfer	O	• Currently no restriction • Changes on the way
Security	O	• All practicable steps to protect personal data • Where 3rd party processor is engaged → contractual / other means required for security and period of retention
Breach Notification	O	• No requirement
DP Officer	O	• No requirement

A Brief Survey: Hong Kong

Regime	*Personal Data (Privacy) Ordinance ("PDPO")*	
Enforcement	O	• Enforcement notices with criminal consequences for non-compliance
Sanction	O	• Fines, criminal convictions and jail sentences
Redress	O	• Private Civil Proceedings
Marketing Activities	O	• Notification • Statement of gain • Free opt-out channel • Consent from Data Subject
Online Privacy	O	• PDPO also applies to online processing • Cookies – use and effect of non-compliance communicated to Data Subject

A Brief Survey: Hong Kong - Aegon Direct …

- *"If the contraventions shown in this case were committed today, the corporate data user at fault would be held criminally liable to a fine and imprisonment …."*

Alan Chiang – Privacy Commissioner

A Brief Survey: Indonesia

Regime	***Law No. 11 of 2008** regarding Electronic Information and Transaction and **Government Regulation No. 82 of 2012** regarding Provision of Electronic System and Transaction*	
Registration	O	• No requirement
Collection & Processing	O	• Consent / other conditions met • Data center – more heavily regulated
Transfer	O	• Data user required to explain control and possession of transmitted information
Security	O	• Data user guarantees protection of personal information • Telecom service provider responsible for data storage
Breach Notification	O	• Required in writing - failure to protect personal data • Report to authority - failure/ disturbance of protection system
DP Officer	O	• No requirement

A Brief Survey: Indonesia

Regime	*Law No. 11 of 2008 regarding Electronic Information and Transaction and Government Regulation No. 82 of 2012 regarding Provision of Electronic System and Transaction*	
Enforcement & Sanctions	O	Imposed under various regulations • Imprisonment and fines • Administrative sanctions (e.g. warning and fines) • Cancellation of approval/ registration
Redress	O	• Private Civil Proceedings
Marketing Activities	O	• No specific regulations • Mostly protected by IP laws
Online Privacy	O	• No specific regulations • Obtain cookies/ location data by unlawful access – imprisonment and fine

A Brief Survey: Japan

Regime	***The Act on the Protection of Personal Information*** *("APPI") and various sector specific guidelines regarding APPI*	
Application	O	• Applies to business operators utilizing a database of 5,000 identifiable individuals on any day in the past 6 months.
Registration	O	• No requirement
Collecting & Processing	O	• Notification of use required. • Public Announcement of Purpose of Use
Transfer	O	• Consent required, unless an exception under APPI applies
Breach Notification	O	• No general requirement under APPI, but specific ministry guidelines provided for business operators
DP Officers	O	• Not required under APPI but required under some guidelines

A Brief Survey: Japan

Regime	***The Act on the Protection of Personal Information*** *("APPI") and various sector specific guidelines regarding APPI*	
Security	O	• Specific guidance set out in Ministry guidelines
Enforcement and Sanctions	O	• Enforcement by relevant Minister – corrective orders • Fines or imprisonment
Redress	O	• No specific right of civil claim under APPI • Contract/ tort claims or injunction can be sought on a case by case basis
Marketing Activities	O	• Act on Specified Commercial Transactions and Act on the Regulation of Transmission of Specified Electronic Mail • Restrictions on email advertisements – prior request or consent required
Online Privacy	O	• No law on cookies • APPI - purpose of Use to be disclosed where information may identify individual
Regime	***The Act on the Protection of Personal Information*** *("APPI"). In addition, various sector specific guidelines regarding APPI.*	

A Brief Survey: Korea

Regime	*Combination of laws – **Personal Information Protection Act** ("PIPA", effective 30/09/11) and **sector specific legislation** (e.g. IT Network Act)*	
Registration	O	• Registration required for "Public institutions"
Collection & Processing	O	• Notification + Consent required • Sensitive personal information - More heavily regulated
Transfer	O	• Notification and Opt-in Consent required
Security	O	• Mandatory security arrangements
Breach Notification	O	• Required in case of leakage/ intrusion/ theft • Report to authority if affected data subjects exceeds 10,000
DP Officer	O	• Require a Designated Data Protection Officer

A Brief Survey: Korea

Regime	*Combination of laws – **Personal Information Protection Act** ("PIPA", effective 30/09/11) and **sector specific legislation** (e.g. IT Network Act)*	
Enforcement	O	• Authorities may request reports on handling of data • Authorities may issue corrective orders
Sanction	O	• Imprisonment and fines
Redress	O	• Statutory right to claim damages from Data User
Marketing Activities	O	• Specify details of the marketing effort • Consent obtained (if market by phone or fax)
Online Privacy	O	• Cookies – opt-out consent required • Automated means of collection – publicize installation, operation and opt-out process • Location information – consent / report to authority

A Brief Survey: Malaysia

Regime	Combination of laws – **Statute/ industry codes/ common law** Personal Data Protection Act (Drafting)	
Registration	O	• No requirement
Collection & Processing	O	• Currently no specific requirements • (Draft PDPA) -- Notification and Consent required
Transfer	O	• Currently no specific requirements • (Draft PDPA) – only allowed for specified jurisdictions
Security	O	• Currently no specific requirements • (Draft PDPA) – "practical" steps of protection
Breach Notification	O	• No requirement
DP Officer	O	• No requirement

DLA PIPER

A Brief Survey: Malaysia

Regime	Combination of laws – **Statute/ industry codes/ common law** Personal Data Protection Act (Drafting)	
Enforcement & Sanctions	O	Currently no specific sanctions Under the Draft PDPA and various laws: • Fines • Suspension/ revocation of telecom license • Criminal penalties
Redress	O	• No specific right of civil claim under Draft PDPA
Marketing Activities	O	• Opt-out option required
Online Privacy	O	• Currently no specific requirements • No specific provisions under Draft PDPA

DLA PIPER

A Brief Survey: Singapore

Regime	*Personal Data Protection Act ("PDPA") formally enacted in January 2013*	
Registration	O	• No requirement
Collection & Processing	O	• Notification + Consent of Data Subject required
Transfer	O	• Allowed if there is comparable standard of protection in destination • Permitted by the Government
Security	O	• Reasonable security arrangements
Breach Notification	O	• No requirement
DP Officer	O	• Required to appoint DP Officer • Contact details must be published

DLA PIPER

A Brief Survey: Singapore

Regime	*Personal Data Protection Act ("PDPA") formally enacted in January 2013*	
Enforcement	O	• Directions of the Commission (notices, fines) → Registrable in Courts and appealable
Sanction	O	• Imprisonment (obstruct/ mislead the Commission)
Redress	O	• Complain to the Commission • Private Civil Proceedings • Investigation by the Commission
Marketing Activities	O	• Phone / text / voice messages →confirm with Do-Not-Call Register • Bulk e-mails / text / MMS messages → specific control
Online Privacy	O	• No specific requirement

A Brief Survey: Taiwan

Regime	*Personal Data Protection Law ("PDPL")*	
Registration	O	• No requirement
Collection & Processing	O	• Notification and Consent / other conditions met
Transfer	O	• No general restrictions • Specific restrictions may be imposed by the Government in certain cases
Security	O	• Proper security measures required
Breach Notification	O	• Required if data stolen/ disclosed/ altered/ infringed
DP Officer	O	• No required in general • Government agencies – specific person in charge of security maintenance

A Brief Survey: Taiwan

Regime	*Personal Data Protection Law ("PDPL")*	
Enforcement	O	• Inspection of protection measures
Sanction	O	• Criminal sanctions • Administrative fines • Civil compensation
Redress	O	• Class action is allowed for civil claims
Marketing Activities	O	• Opt-out option to Data Subjects
Online Privacy	O	• No specific regulations

A Brief Survey: Thailand

Regime	*Combination of laws – **Constitution of Thailand/ Thai Penal Code/ Child Protection Act** Personal Information Protection Act (Drafting)*	
Registration	*Combination of laws – **Constitution of Thailand/ Thai Penal Code/ Child Protection Act** Personal Information Protection Act (Drafting)*	
Collection & Processing	O	• No requirement
Transfer	O	• Consent / other conditions met
Security	O	• Consent required in general • Wrongful if causes damage to Data Subject
Breach Notification	O	• Specific Businesses – maintain level of security • Non-Specific businesses – prevention of unauthorized access
DP Officer	O	• No requirement

A Brief Survey: Thailand

Regime	*Combination of laws – **Constitution of Thailand/ Thai Penal Code/ Child Protection Act** Personal Information Protection Act (Drafting)*	
Enforcement & Sanctions	O	Imposed under various regulations • Fines • Suspension/ revocation of telecom license • Criminal penalties
Redress	O	• Private Civil Proceedings
Marketing Activities	O	• No specific regulations
Online Privacy	O	• No specific regulations • Punishment for computer data alterations

A Brief Survey: Philippines

Regime	*New law passed on 15 August 2012, based on EU Directive 95/46/EC*	
Registration	O	• No requirement
Collection & Processing	O	• Notification + Consent / other conditions met • Sensitive personal information - More heavily regulated
Transfer	O	Permitted if: • For legitimate purposes • Controller remains responsible
Security	O	• Mandatory security arrangements (responsible for third parties' processing on one's behalf) • Confidentiality obligation extends to employees and agents
Breach Notification	O	• Sensitive information breaches • Information accessed may enable identity fraud
DP Officer	O	• Required to appoint DP Officer • Contact details must be published

A Brief Survey: Philippines

Regime	*New law passed on 15 August 2012, based on EU Directive 95/46/EC*	
Enforcement	O	Various sanctions by the Commission (cease and desist orders, ban on processing, investigation and reports, etc)
Sanction	O	Imprisonment and fines
Redress	O	• Complain to the Commission • Private Civil Proceedings • Investigation by the Commission
Marketing Activities	O	• Clear description of products/ transactions + • Consent obtained/ existing customers/ opt-out options
Online Privacy	O	• Criminal penalty on computer crimes • Authorities can collect or record traffic data transmitted by means of computer system

A Brief Survey: Vietnam

Regime	*Combination of laws – **Vietnam Constitution/ Civil code/ Law on Protection of Consumers Right/ Law on E-Transactions/ Law on Insurance Business/ Law on Information Technology*** *Information Safety Law (Drafting)*	
Registration	O	• No requirement
Collection & Processing	O	• Notification + Consent required
Transfer	O	• Consent required to transfer to a third party but no specific restrictions on overseas transfer of personal data
Security	O	• Necessary security arrangements
Breach Notification	O	• No requirement
DP Officer	O	• No requirement

DLA PIPER

A Brief Survey: Vietnam

Regime	*Combination of laws – **Vietnam Constitution/ Civil code/ Law on Protection of Consumers Right/ Law on E-Transactions/ Law on Insurance Business/ Law on Information Technology*** *Information Safety Law (Drafting)*	
Enforcement & Sanction	O	• Administrative fines • Criminal penalties
Redress	O	• Statutory right to demand or request for compensation
Marketing Activities	O	• Specify requirements for sending advertising emails/text messages/fax + • Consent required
Online Privacy	O	• No specific regulation on the use of cookies • Subject to other laws if cookies are used to collect personal data

What are we seeing?

Consistent observation: Not ready / as ready

Resource commitment

Outward signs:

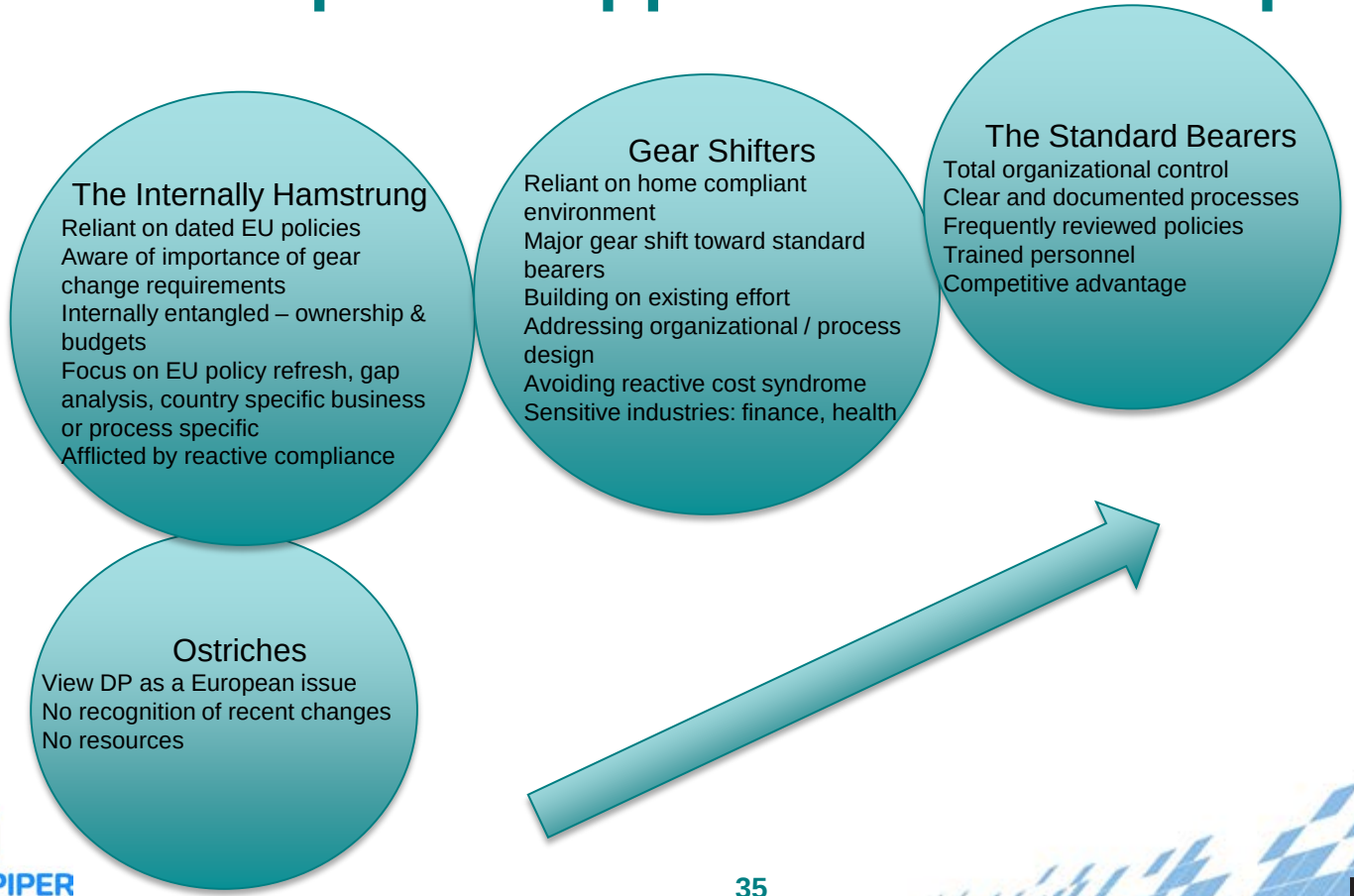
- Fewer privacy professionals in region
- High turnover of privacy professionals
- Confused compliance ownership
- Reliance on home jurisdiction derived policies
- Policy maintenance
- Undocumented compliance strategy
- Reliance on key man solutions

Awareness

Common issues:

- Rate/state of development
- Specific local nuances
- Application
- Consequences/personal liability
- Extra-territorial impact
- Effective risk allocation
- Marketing restrictions
- Workplace compliance culture
- External support inefficient

Different corporate approaches to data protection



Your Readiness

- Which category do you fall into?
- Do some of our clients challenges resonate with you?
- Does each business you operate in Asia have its own privacy rep?
- Have your policies been calibrated to regional changes and differences?
- Have you audited regional compliance levels recently?

Asia Pac Enforcement Conclusions

- General increase in enforcement actions and level of fines
- Explosive growth in new laws
- New enforcement in "green field" countries
- Regulators given more responsibilities and authority to impose higher fines
- Increased breach notification requirements (e.g. Japan, possibly Australia)
- Requirement for greater accountability
- External factors (e.g. Cyber crimes/Data breaches on the rise)