



# CYBER SECURITY - CYBER RISK MANAGEMENT AND MITIGATION

*Scott Thiel, Partner  
June 2015*

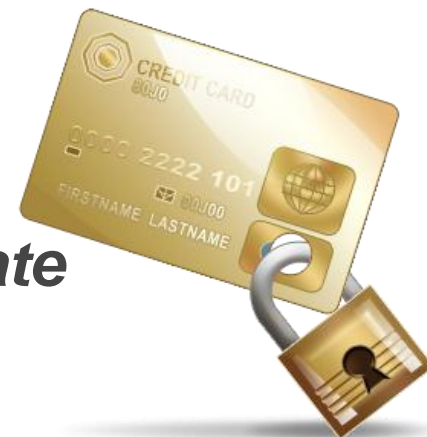
## TECHLAW AUSTRALIA 2015

1. Current threat environment
2. Regulatory frameworks of countries in the Asia Pacific region
3. Key challenges and practical issues for multinational business
4. Asia Pacific enforcement conclusions

- 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*



- 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:

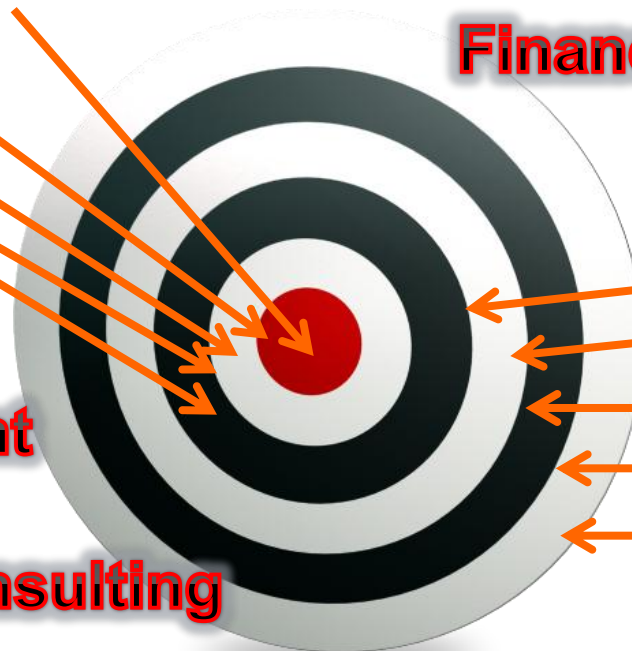
1. South Korea
2. Japan
3. Taiwan
4. Thailand
5. Hong Kong

**Government**

**Consulting**

**Finance/ Banking**

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



- Data Breaches exposed weak defences of organisations in the Asia Pacific region

**Callbacks**

**System Infection**

**Data Exfiltration**

**Malware**

- 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

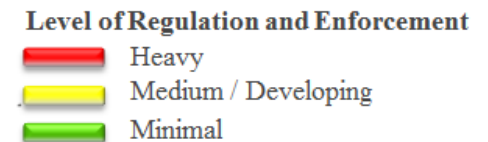
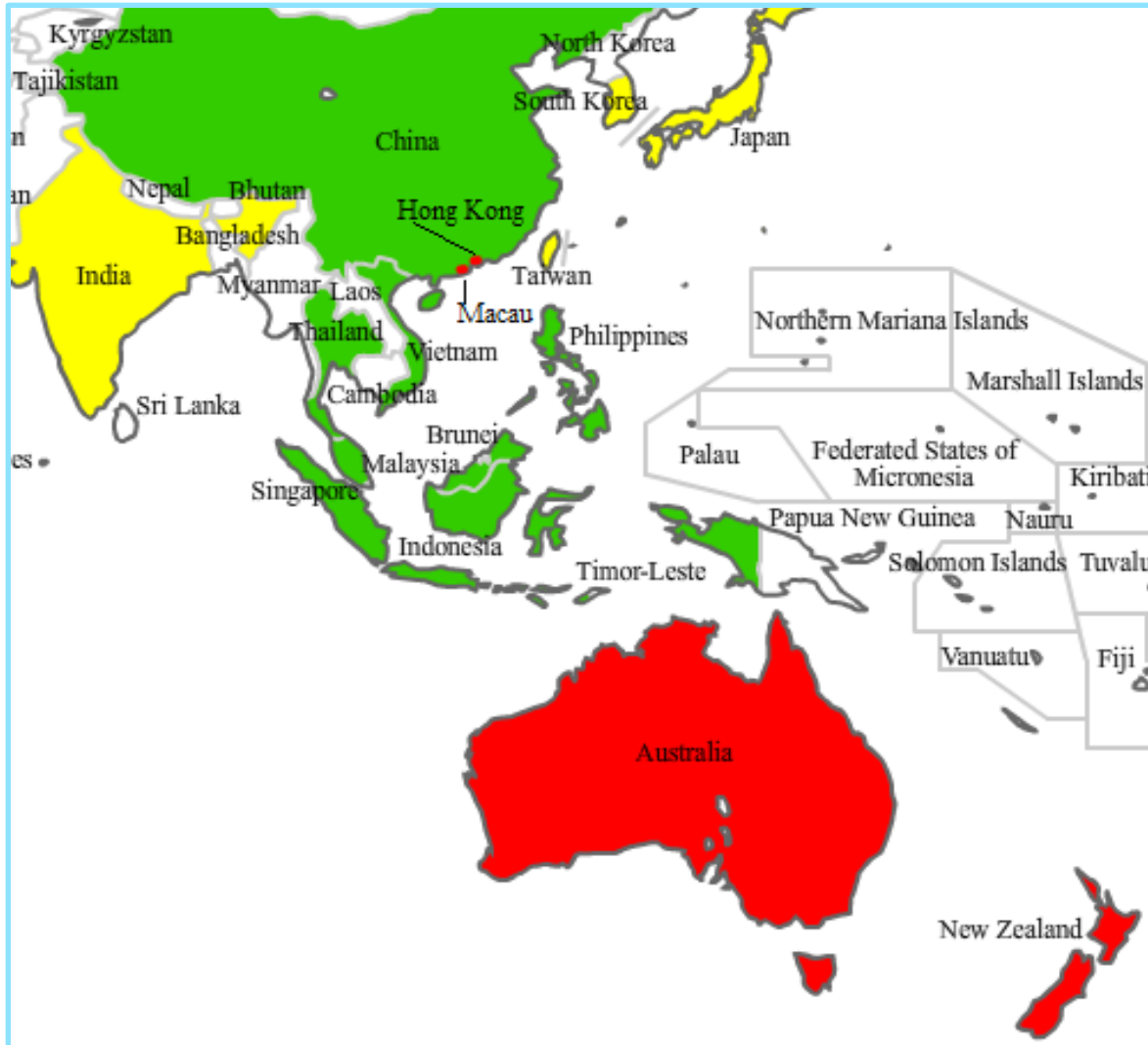
Exponential growth of information

Growing protection challenge

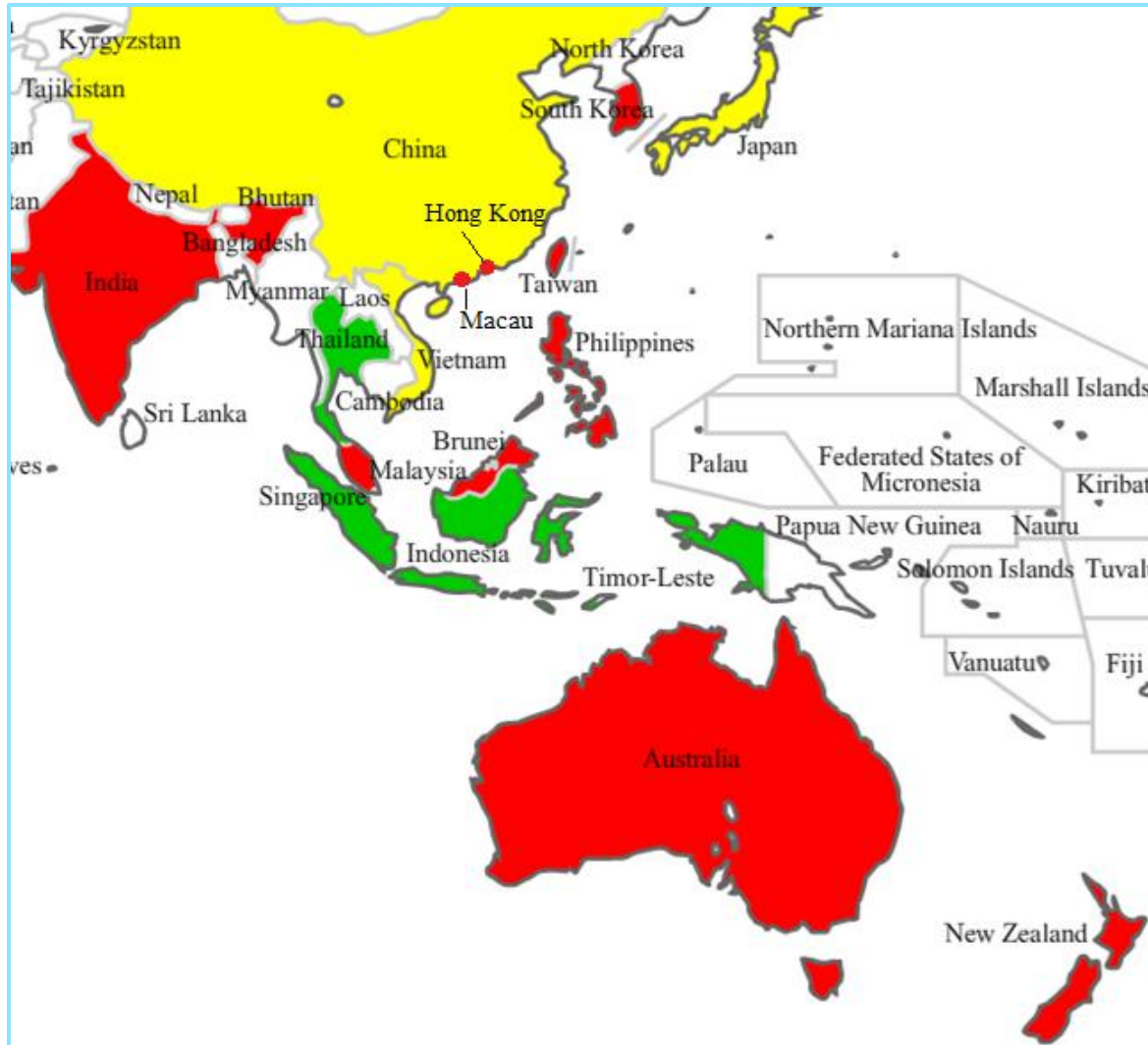
Corporate requirements and privacy collide

Data and information breaches/disputes  
- High cost of mistakes

## Before (2011)



At 2014

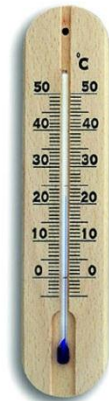


**Level of Regulation and Enforcement**

- Heavy
- Medium / Developing
- Minimal






- **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 (Shah's report\*)



# Asia- Pacific Data Protection: Harmonisation?

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

**Level of Regulation and Enforcement**

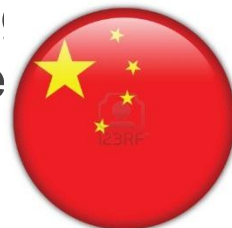
-  Heavy
-  Medium / Developing
-  Minimal



- **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



- **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 Infringement of Personal Rights and Interests through the Inte





Regime	<i>Personal Data (Privacy) Ordinance ("PDPO")</i>	
<b>Registration</b>	○	➤ No requirement
<b>Collection &amp; Processing</b>	○	<ul style="list-style-type: none"> <li>➤ <u>Notification</u> + <u>Consent</u> (for new purpose) of Data Subject</li> <li>➤ New <u>Consent</u> requirements for direct marketing commence 1 April 2013</li> </ul>
<b>Transfer</b>	○	<ul style="list-style-type: none"> <li>➤ Currently no restriction</li> <li>➤ Changes on the way</li> </ul>
<b>Security</b>	○	<ul style="list-style-type: none"> <li>➤ All practicable steps to protect personal data</li> <li>➤ Where 3<sup>rd</sup> party processor is engaged → contractual / other means required for security and period of retention</li> </ul>
<b>Breach Notification</b>	○	➤ No requirement
<b>DP Officer</b>	○	➤ No requirement



Regime	<i>Personal Data (Privacy) Ordinance ("PDPO")</i>	
<b>Enforcement</b>	○	➤ Enforcement notices with criminal consequences for non-compliance
<b>Sanction</b>	○	➤ Fines, criminal convictions and jail sentences
<b>Redress</b>	○	➤ Private Civil Proceedings
<b>Marketing Activities</b>	○	<ul style="list-style-type: none"> <li>➤ Notification</li> <li>➤ Statement of gain</li> <li>➤ Free opt-out channel</li> <li>➤ Consent from Data Subject</li> </ul>
<b>Online Privacy</b>	○	<ul style="list-style-type: none"> <li>➤ PDPO also applies to online processing</li> <li>➤ Cookies – use and effect of non-compliance communicated to Data Subject</li> </ul>



- *"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

<b>Regime</b>	<i>Law No. 11 of 2008 regarding Electronic Information and Transaction and <b>Government Regulation No. 82 of 2012 regarding Provision of Electronic System and Transaction</b></i>	
<b>Registration</b>	○	No requirement
<b>Collection &amp; Processing</b>	○	<ul style="list-style-type: none"> <li>➤ <u>Consent / other conditions</u> met</li> <li>➤ Data center – more heavily regulated</li> </ul>
<b>Transfer</b>	○	Data user required to explain control and possession of transmitted information
<b>Security</b>	○	<ul style="list-style-type: none"> <li>➤ Data user guarantees protection of personal information</li> <li>➤ Telecom service provider responsible for data storage</li> </ul>
<b>Breach Notification</b>	○	<ul style="list-style-type: none"> <li>➤ Required in writing - failure to protect personal data</li> <li>➤ Report to authority - failure/ disturbance of protection system</li> </ul>
<b>DP Officer</b>	○	No requirement



<b>Regime</b>	<i>Law No. 11 of 2008 regarding Electronic Information and Transaction and <b>Government Regulation No. 82 of 2012 regarding Provision of Electronic System and Transaction</b></i>	
<b>Enforcement &amp; Sanctions</b>	○	<ul style="list-style-type: none"> <li>Imposed under various regulations               <ul style="list-style-type: none"> <li>➤ Imprisonment and fines</li> <li>➤ Administrative sanctions (e.g. warning and fines)</li> <li>➤ Cancellation of approval/ registration</li> </ul> </li> </ul>
<b>Redress</b>	○	<ul style="list-style-type: none"> <li>➤ Private Civil Proceedings</li> </ul>
<b>Marketing Activities</b>	○	<ul style="list-style-type: none"> <li>➤ No specific regulations</li> <li>➤ Mostly protected by IP laws</li> </ul>
<b>Online Privacy</b>	○	<ul style="list-style-type: none"> <li>➤ No specific regulations</li> <li>➤ Obtain cookies/ location data by unlawful access – imprisonment and fine</li> </ul>





<b>Regime</b>	<i>The Act on the Protection of Personal Information ("APPI") and various sector specific guidelines regarding APPI</i>	
<b>Application</b>	○	➤ Applies to business operators utilizing a database of 5,000 identifiable individuals on any day in the past 6 months.
<b>Registration</b>	○	➤ No requirement
<b>Collecting &amp; Processing</b>	○	<ul style="list-style-type: none"> <li>➤ Notification of use required.</li> <li>➤ Public Announcement of Purpose of Use</li> </ul>
<b>Transfer</b>	○	➤ Consent required, unless an exception under APPI applies
<b>Breach Notification</b>	○	➤ No general requirement under APPI, but specific ministry guidelines provided for business operators
<b>DP Officers</b>	○	➤ Not required under APPI but required under some guidelines



<b>Regime</b>	<i>The Act on the Protection of Personal Information ("APPI"). In addition, various sector specific guidelines regarding APPI.</i>	
<b>Security</b>	○	➤ Specific guidance set out in Ministry guidelines
<b>Enforcement and Sanctions</b>	○	<ul style="list-style-type: none"> <li>➤ Enforcement by relevant Minister – corrective orders</li> <li>➤ Fines or imprisonment</li> </ul>
<b>Redress</b>	○	<ul style="list-style-type: none"> <li>➤ No specific right of civil claim under APPI</li> <li>➤ Contract/ tort claims or injunction can be sought on a case by case basis</li> </ul>
<b>Marketing Activities</b>	○	<ul style="list-style-type: none"> <li>➤ Act on Specified Commercial Transactions and Act on the Regulation of Transmission of Specified Electronic Mail</li> <li>➤ Restrictions on email advertisements – prior request or consent required</li> </ul>
<b>Online Privacy</b>	○	<ul style="list-style-type: none"> <li>➤ No law on cookies</li> <li>➤ APPI - purpose of Use to be disclosed where informa identify individual</li> </ul>



<b>Regime</b>	<i>Combination of laws – <b>Personal Information Protection Act</b> ("PIPA", effective 30/09/11) and <b>sector specific legislation</b> (e.g. IT Network Act)</i>	
<b>Registration</b>	○	Registration required for "Public institutions"
<b>Collection &amp; Processing</b>	○	<u>Notification</u> + <u>Consent</u> required Sensitive personal information - More heavily regulated
<b>Transfer</b>	○	<u>Notification</u> and <u>Opt-in Consent</u> required
<b>Security</b>	○	Mandatory security arrangements
<b>Breach Notification</b>	○	<ul style="list-style-type: none"> <li>➤ Required in case of leakage/ intrusion/ theft</li> <li>➤ Report to authority if affected data subjects exceeds 10,000</li> </ul>
<b>DP Officer</b>	○	Require a Designated Data Protection Officer



<b>Regime</b>	<i>Combination of laws – <b>Personal Information Protection Act</b> ("PIPA", effective 30/09/11) and <b>sector specific legislation</b> (e.g. IT Network Act)</i>	
<b>Enforcement</b>	○	<ul style="list-style-type: none"> <li>➤ Authorities may request reports on handling of data</li> <li>➤ Authorities may issue corrective orders</li> </ul>
<b>Sanction</b>	○	Imprisonment and fines
<b>Redress</b>	○	Statutory right to claim damages from Data User
<b>Marketing Activities</b>	○	<ul style="list-style-type: none"> <li>➤ Specify details of the marketing effort</li> <li>+</li> <li>➤ Consent obtained (if market by phone or fax)</li> </ul>
<b>Online Privacy</b>	○	<ul style="list-style-type: none"> <li>➤ Cookies – opt-out consent required</li> <li>➤ Automated means of collection – publicize installation, operation and opt-out process</li> <li>➤ Location information – consent / report to authority</li> </ul>



<b>Regime</b>	Combination of laws – <b>Statute/ industry codes/ common law</b> Personal Data Protection Act (Drafting)	
<b>Registration</b>	○	No requirement
<b>Collection &amp; Processing</b>	○	<ul style="list-style-type: none"> <li>➤ Currently no specific requirements</li> <li>➤ (Draft PDPA) -- Notification and Consent required</li> </ul>
<b>Transfer</b>	○	<ul style="list-style-type: none"> <li>➤ Currently no specific requirements</li> <li>➤ (Draft PDPA) – only allowed for specified jurisdictions</li> </ul>
<b>Security</b>	○	<ul style="list-style-type: none"> <li>➤ Currently no specific requirements</li> <li>➤ (Draft PDPA) – "practical" steps of protection</li> </ul>
<b>Breach Notification</b>	○	No requirement
<b>DP Officer</b>	○	No requirement





<b>Regime</b>	Combination of laws – <b>Statute/ industry codes/ common law</b> Personal Data Protection Act (Drafting)	
<b>Enforcement &amp; Sanctions</b>	○	<p>Currently no specific sanctions Under the Draft PDPA and various laws:</p> <ul style="list-style-type: none"> <li>➤ Fines</li> <li>➤ Suspension/ revocation of telecom license</li> <li>➤ Criminal penalties</li> </ul>
<b>Redress</b>	○	➤ No specific right of civil claim under Draft PDPA
<b>Marketing Activities</b>	○	➤ Opt-out option required
<b>Online Privacy</b>	○	<ul style="list-style-type: none"> <li>➤ Currently no specific requirements</li> <li>➤ No specific provisions under Draft PDPA</li> </ul>



<b>Regime</b>	<i>Personal Data Protection Act ("PDPA") formally enacted in January 2013</i>	
<b>Registration</b>	○	No requirement
<b>Collection &amp; Processing</b>	○	<u>Notification</u> + <u>Consent</u> of Data Subject required
<b>Transfer</b>	○	<ul style="list-style-type: none"> <li>➤ Allowed if there is comparable standard of protection in destination</li> <li>➤ Permitted by the Government</li> </ul>
<b>Security</b>	○	Reasonable security arrangements
<b>Breach Notification</b>	○	No requirement
<b>DP Officer</b>	○	<ul style="list-style-type: none"> <li>➤ Required to appoint DP Officer</li> <li>➤ Contact details must be published</li> </ul>



<b>Regime</b>	<i>Personal Data Protection Act ("PDPA") formally enacted in January 2013</i>	
<b>Enforcement</b>	○	<u>Directions</u> of the Commission (notices, fines) → Registrable in Courts and appealable
<b>Sanction</b>	○	Imprisonment (obstruct/ mislead the Commission)
<b>Redress</b>	○	<ul style="list-style-type: none"> <li>➤ Complain to the Commission</li> <li>➤ Private Civil Proceedings</li> <li>➤ Investigation by the Commission</li> </ul>
<b>Marketing Activities</b>	○	<ul style="list-style-type: none"> <li>➤ Phone / text / voice messages → confirm with <u>Do-Not-Call Register</u></li> <li>➤ Bulk e-mails / text / MMS messages → specific control</li> </ul>
<b>Online Privacy</b>	○	No specific requirement



Regime	<i>Personal Data Protection Law ("PDPL")</i>	
<b>Registration</b>	○	No requirement
<b>Collection &amp; Processing</b>	○	<u>Notification</u> and <u>Consent</u> / <u>other conditions</u> met
<b>Transfer</b>	○	<ul style="list-style-type: none"> <li>➤ No general restrictions</li> <li>➤ Specific restrictions may be imposed by the Government in certain cases</li> </ul>
<b>Security</b>	○	Proper security measures required
<b>Breach Notification</b>	○	Required if data stolen/ disclosed/ altered/ infringed
<b>DP Officer</b>	○	<ul style="list-style-type: none"> <li>➤ No required in general</li> <li>➤ Government agencies – specific person in charge of security maintenance</li> </ul>



Regime	<i>Personal Data Protection Law ("PDPL")</i>	
<b>Enforcement</b>	○	➤ Inspection of protection measures
<b>Sanction</b>	○	<ul style="list-style-type: none"> <li>➤ Criminal sanctions</li> <li>➤ Administrative fines</li> <li>➤ Civil compensation</li> </ul>
<b>Redress</b>	○	➤ Class action is allowed for civil claims
<b>Marketing Activities</b>	○	➤ Opt-out option to Data Subjects
<b>Online Privacy</b>	○	➤ No specific regulations





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



<b>Regime</b>	<i>Combination of laws – <b>Constitution of Thailand/ Thai Penal Code/ Child Protection Act</b> Personal Information Protection Act (Drafting)</i>	
<b>Enforcement &amp; Sanctions</b>	○	<ul style="list-style-type: none"> <li>➤ Imposed under various regulations</li> <li>➤ Fines</li> <li>➤ Suspension/ revocation of telecom license</li> <li>➤ Criminal penalties</li> </ul>
<b>Redress</b>	○	<ul style="list-style-type: none"> <li>➤ Private Civil Proceedings</li> </ul>
<b>Marketing Activities</b>	○	<ul style="list-style-type: none"> <li>➤ No specific regulations</li> </ul>
<b>Online Privacy</b>	○	<ul style="list-style-type: none"> <li>➤ No specific regulations</li> <li>➤ Punishment for computer data alterations</li> </ul>



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



<b>Regime</b>	<i>New law passed on 15 August 2012, based on EU Directive 95/46/EC</i>	
<b>Enforcement</b>	○	Various sanctions by the Commission (cease and desist orders, ban on processing, investigation and reports, etc)
<b>Sanction</b>	○	Imprisonment and fines
<b>Redress</b>	○	<ul style="list-style-type: none"> <li>➤ Complain to the Commission</li> <li>➤ Private Civil Proceedings</li> <li>➤ Investigation by the Commission</li> </ul>
<b>Marketing Activities</b>	○	<ul style="list-style-type: none"> <li>➤ Clear description of products/ transactions</li> <li>+</li> <li>➤ Consent obtained/ existing customers/ opt-out options</li> </ul>
<b>Online Privacy</b>	○	<ul style="list-style-type: none"> <li>➤ Criminal penalty on computer crimes</li> <li>➤ Authorities can collect or record traffic data transmitted by means of computer system</li> </ul>



<b>Regime</b>	<i>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)</i>	
<b>Registration</b>	<input checked="" type="radio"/>	No requirement
<b>Collection &amp; Processing</b>	<input type="radio"/>	<u>Notification</u> + <u>Consent</u> required
<b>Transfer</b>	<input type="radio"/>	Consent required to transfer to a third party but no specific restrictions on overseas transfer of personal data
<b>Security</b>	<input type="radio"/>	➤ Necessary security arrangements
<b>Breach Notification</b>	<input checked="" type="radio"/>	No requirement
<b>DP Officer</b>	<input checked="" type="radio"/>	No requirement



<b>Regime</b>	<i>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)</i>	
<b>Enforcement &amp; Sanction</b>	○	<ul style="list-style-type: none"> <li>➤ Administrative fines</li> <li>➤ Criminal penalties</li> </ul>
<b>Redress</b>	○	Statutory right to demand or request for compensation
<b>Marketing Activities</b>	○	<ul style="list-style-type: none"> <li>➤ Specify requirements for sending advertising emails/text messages/fax</li> <li>+</li> <li>➤ Consent required</li> </ul>
<b>Online Privacy</b>	○	<ul style="list-style-type: none"> <li>➤ No specific regulation on the use of cookies</li> <li>➤ Subject to other laws if cookies are used to collect personal data</li> </ul>





## Consistent observation: Not ready / as ready

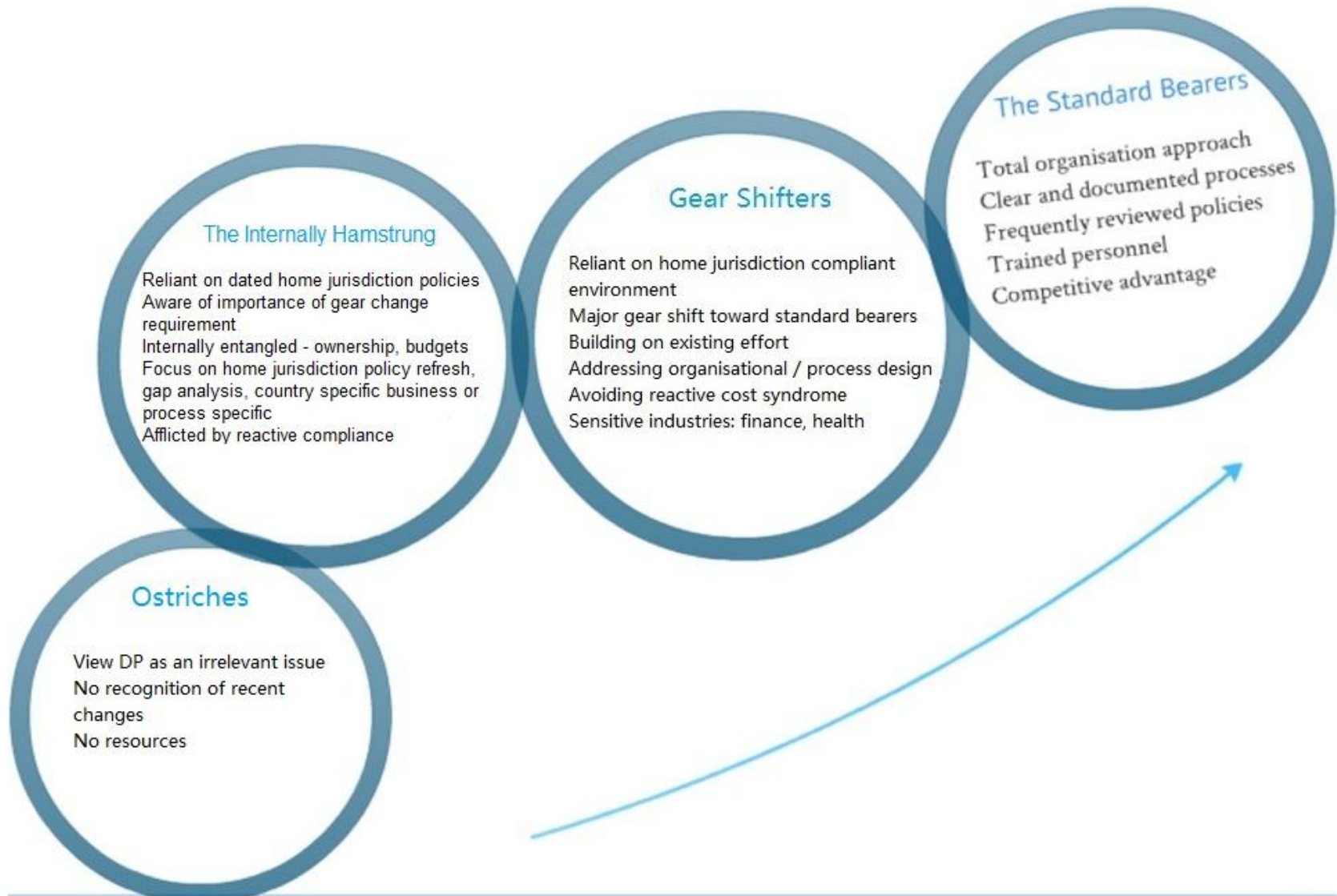
### Resource commitment

- 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

# The different corporate approaches to data protection



- 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?

- 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)