


DATA RISK MANAGEMENT BAROMETER

GAUGING ASIA-PACIFIC'S POTENTIAL

IT PRIORITIES AND DATA MANAGEMENT CHALLENGES

The IDC C-Suite Barometer identified the top 3 CXO IT Priorities:



Building a more secure IT environment



Improving or simplifying IT infrastructure via optimization



Enabling business innovations

Balancing these are 3 key challenges:



Cyber threats such as ransomware



Business disruption



Competition from new business models

ASIA-PACIFIC DATA RISK MANAGEMENT BAROMETER

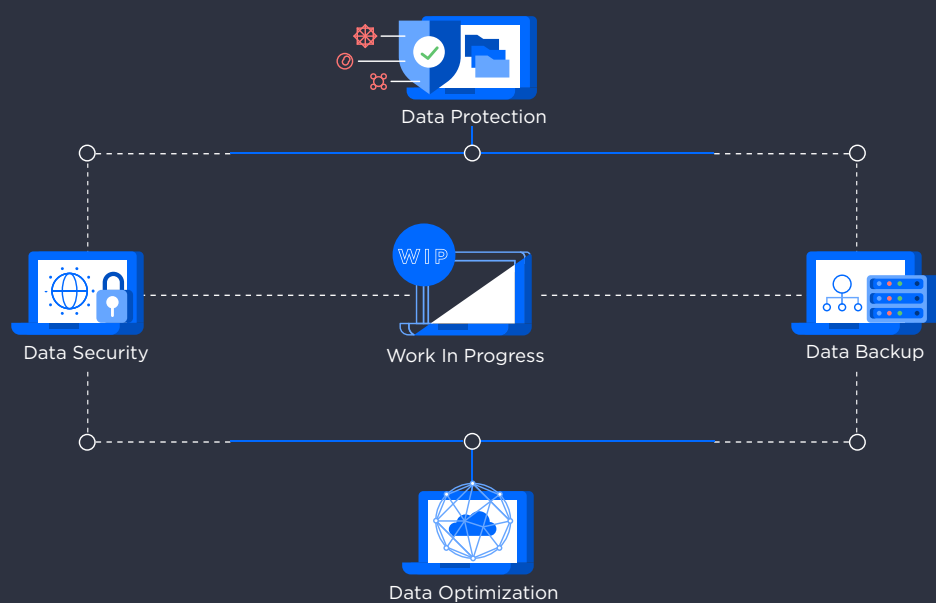
	COUNTRIES	MAXIMUM PENALTY THAT MAY BE IMPOSED IN LOCAL CURRENCY
HIGH RISK MANAGEMENT	01 SINGAPORE	SGD 1,000,000
	02 AUSTRALIA	AUD 1,700,000
	03 HONG KONG	HKD 1,000,000
	04 INDONESIA	IDR 5,000,000,000
	05 MALAYSIA	MYR 300,000
	06 PHILIPPINES	PHP 2,000,000
LOW RISK MANAGEMENT	07 TAIWAN	TWD 1,000,000
	08 NEW ZEALAND	NZD 10,000
	09 KOREA	KRW 50,000,000
	10 VIETNAM	VND 140,000
	11 CHINA	CNY 1,000,000
	12 JAPAN	JPY 1,000,000
	13 INDIA	INR 500,000
	14 THAILAND	NA

This barometer shows a ranking of 14 markets across the Asia-Pacific region, from the strictest to the seemingly indifferent, in terms of the **financial penalty that may be imposed for breach of data privacy as a percentage of the country's GDP.**

Based on research available publicly Singapore appears to have the highest amount of financial penalty that can be imposed on corporations, closely followed by Australia. For these six markets at the bottom, the percentage of GDP is almost insignificant, although Korea and Japan can also impose a prison sentence. Thailand has yet to impose any form of legislative penalty.

Regulatory and compliance information is as at 30 June 2017 obtained from publicly available local government Web sites and may not be a complete summary of all applicable laws in the jurisdiction. Information in this study not independently verified or guaranteed by Dell EMC.


BUSINESS CONTINUITY PLANNING IS STILL WORK IN PROGRESS



Business continuity planning (BCP) affects the availability of data by ensuring its availability as much as possible and is about how effectively operations can be recovered without losing the data.

Non-compulsory guidelines and BCP best practices are available in most countries in the region. So far, most countries do not have legislation that address this.

ACTIONS TO LIMIT EXPOSURE SIX KEY AREAS

<p>ONE</p>  <p>Integrity of data and access to data are critical components of a robust data management practice.</p>	<p>TWO</p>  <p>Whether on- or off-premises, on or offshore — management requirements are the responsibility of both the data owner and the data processor.</p>	<p>THREE</p>  <p>In this new world, data recovery (from backup) is going to become more critical over time.</p>	<p>FOUR</p>  <p>To protect your business from cyberattacks/ ransomware, use air-gap solutions with faster restore capabilities for business critical functions.</p>	<p>FIVE</p>  <p>Recovery Point and Recovery Time Objectives will need to be near to zero as possible to be a successful business.</p>	<p>SIX</p>  <p>Since "data is the new oil", visibility into what data is located where, will become more important in order to be secure, compliant and to be able to monetize data more effectively.</p>
---	--	---	---	---	---