MARSH & McLENNAN COMPANIES

CYBER – WHY ARE WE STRUGGLING TO MANAGE EXPOSURES

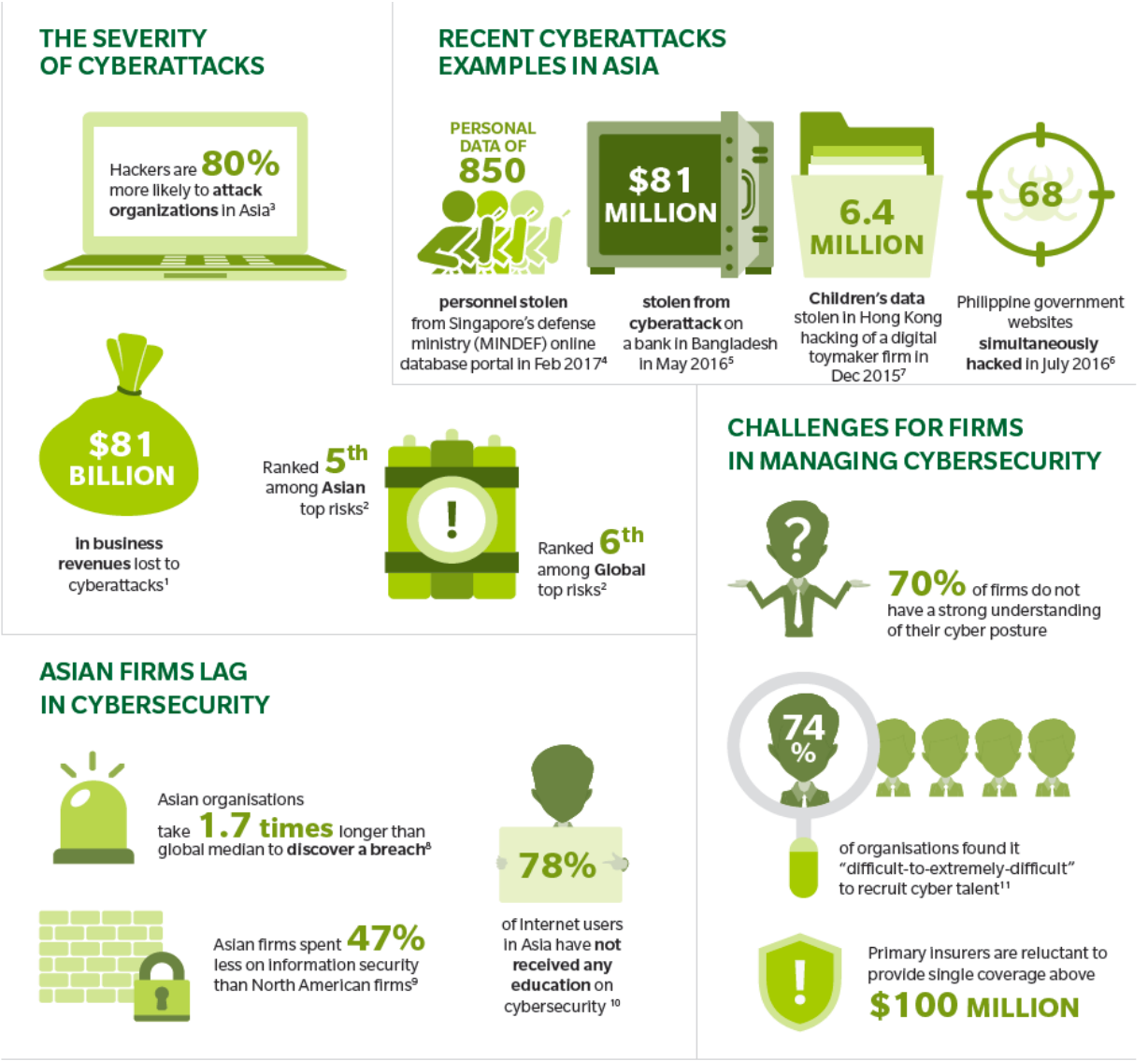
MARCH 2017

Douglas Ure
Managing Director
Marsh Risk Consulting

1 Introduction and motivation

The global cyber risk landscape today

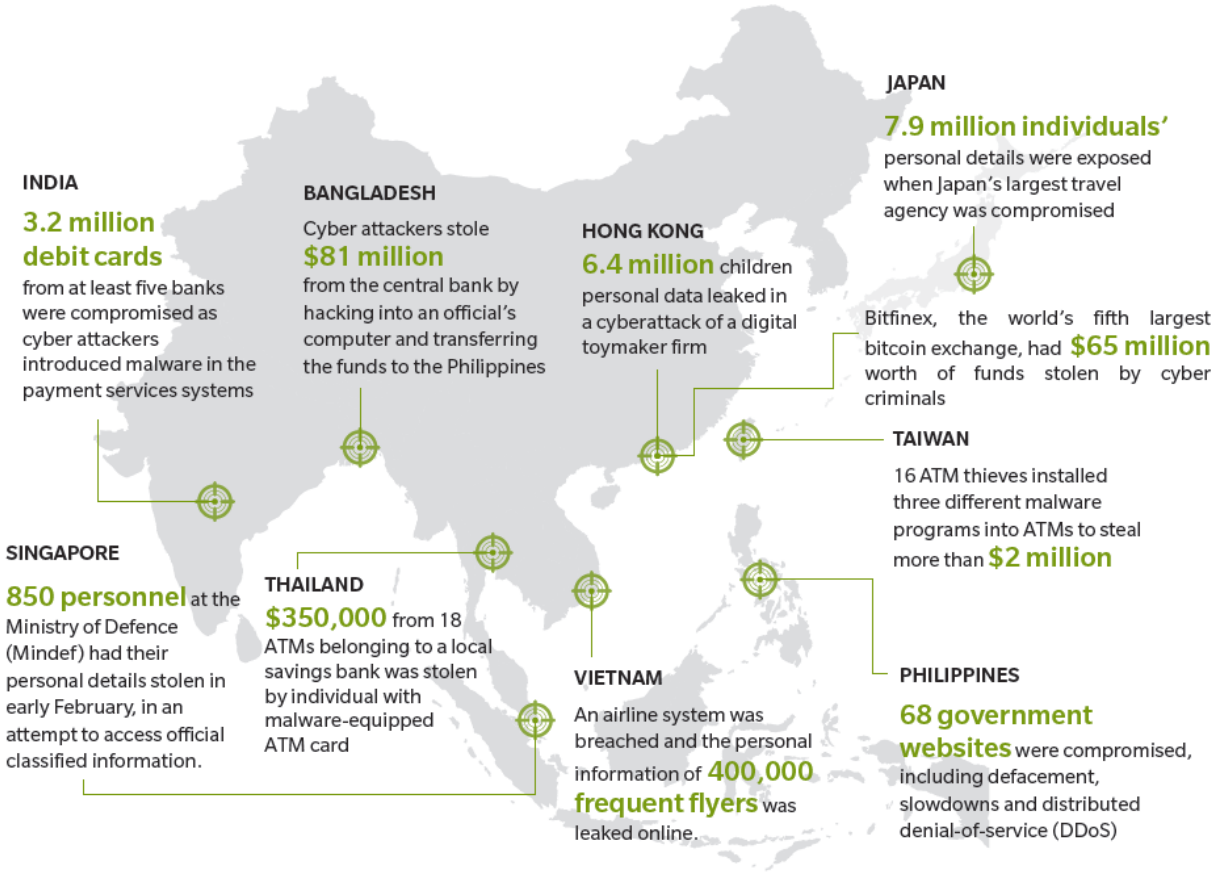
Severity of cyberattacks in APAC is much greater but Asian companies are still lagging the West in cybersecurity



Source: APRC analysis

APAC is a prime target for cybercrimes

Underestimated by reported incidents due to inadequate breach notification laws



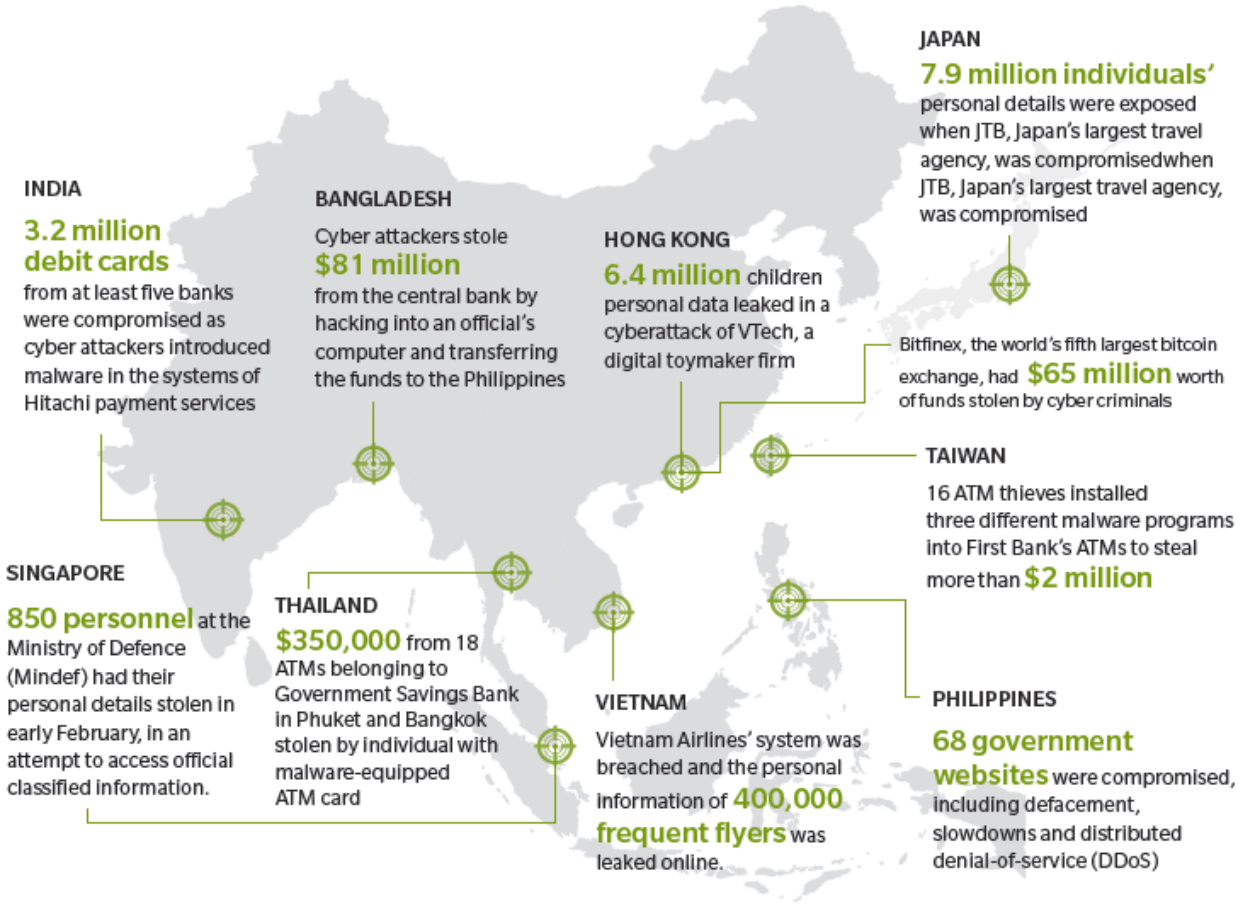
Source: APRC analysis

Recent cyberattacks in APAC

- Reported incidents represent only a handful of all attacks
- LogRhythm estimated up to **90% of APAC companies** are subjected to some form of cyberattack in 2016
- **$81.3 Bn revenues lost** to cyberattacks in APAC in 2015:
  - 25% of global total of $315 Bn
  - Double that of North America and Europe combined ($40 Bn)

Asia is a prime target for cybercrimes

Underestimated by reported incidents due to inadequate breach notification laws



Source: APRC analysis

Recent cyberattacks in APAC

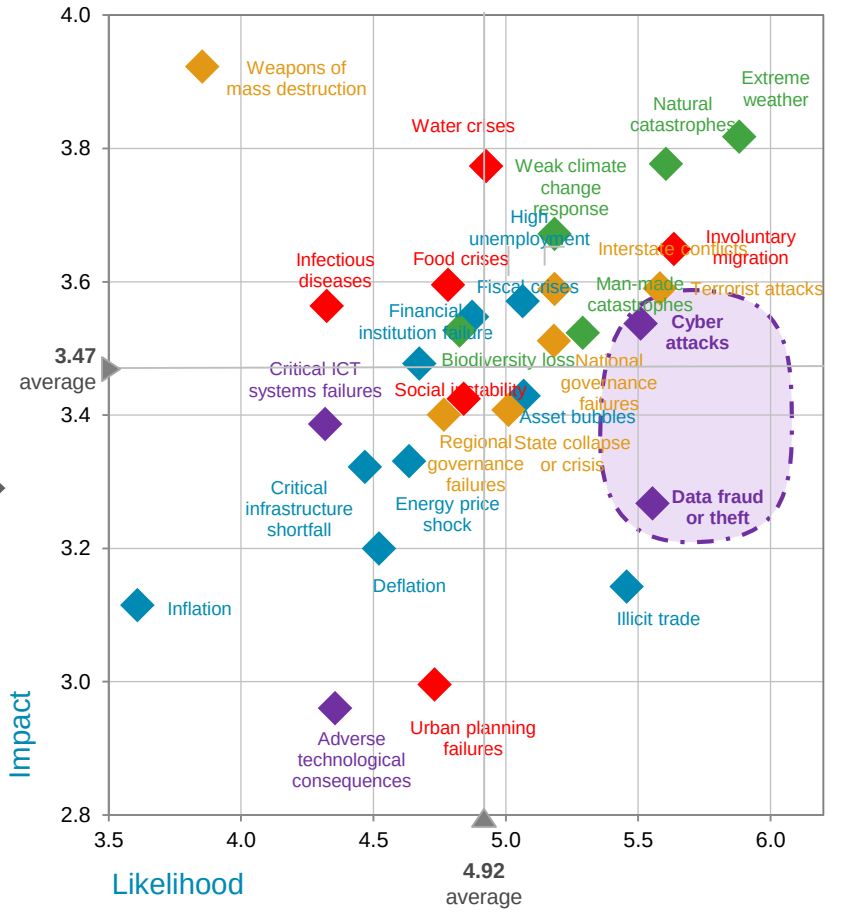
- Reported incidents represent only a handful of all attacks
- LogRhythm estimated up to **90% of APAC companies** are subjected to some form of cyberattack in 2016
- **$81.3 Bn revenues lost** to cyberattacks in APAC in 2015:
  - 25% of global total of $315 Bn
  - Double that of North America and Europe combined ($40 Bn)

Global risk trends
Cyber risks are among the likeliest and most severe in the world

Current cyber risk assessment

- **Rising cyber dependency** is among top 5 risk trends determining global developments
- Cyber risk is **entrenched in daily operations** of organizations across all industries and geographies
  - Cost of data breaches est. **$2.1 trillion** by 2019
  - More than 4X that in 2015
- As a result, data fraud and cyberattacks are ranked **6th highest global risks** in terms of likelihood over the next decade[1]
- Growing global awareness but **lacking decisive mitigation actions** by companies

WEF Global Risks 2017 Landscape[1]



1. Source: World Economic Forum, Global Risks Report 2017

Ever-present ever-growing cyber threat
Asia is 80% greater likelihood of cybercrime target than rest of the world

Accelerating digital transformation in Asia

- Asia strong economic growth powered by **rapid adoption of Internet and mobile technologies**
  - Myanmar is now 20% online, according to the World Bank, compared to less than 2% in 2013.
  - Indonesia mobile subscription rates are the highest in APAC (132% vs 104%).
  - Unfortunately, there is hardly any legislation against cyber crimes in these countries.

Expanding sources of vulnerability via IoTs

- **Asia leads** in the IoT technology:
  - South Korea (#2), Australia (#4), and Japan (#5) tops the 2016 IDC "*Internet-of-Things Index*"
  - China, Japan, and South Korea constantly looking to "*smartify*" consumer electronics with intelligence
- Higher interconnectivity **widens range of vulnerabilities** due to poor or non-existent security features:
  - One of Singapore's major broadband network, suffered a DDoS attack through vulnerabilities exposed via compromised personal IoT devises (webcams and routers), causing two waves of network outage

Ever-present ever-growing cyber threat

Asia is 80% greater likelihood of cybercrime target than rest of the world – a perfect cyber storm?

Speed of digital transformation

MORE INTERNET USERS GLOBALLY[1]

3.7 billion
in 2016

4.2 billion
in 2020; growth led by APAC (60%)

GREATER INTERCONNECTIVITY AMONG 4G MOBILE DEVICES[2]

1 billion
(connections) in 2015

4.7 billion
in 2020; almost ½ (49%) of the increase attributed to APAC

HIGHER MOBILE NETWORK TRAFFIC[3]

7EB/mth
in 2016

35EB/mth
in 2020; APAC accounts for the largest share of traffic (47%)

APAC leads the Internet-of-Things (IoTs) market

TECHNOLOGY ADOPTION PIONEERS[4]
Japan and South Korea pioneered the adoption of IoT and machine-to-machine technology

TOP BROADBAND (INTERNET) SPEED

27 Mbps **19.5 Mbps**[5,6]

compared to global average of
5.6 Mbps

GLOBAL IOT CONNECTIVITY[7]

4.9 billion
(units) in 2015

25 billion
in 2020; with APAC contributing 8.6 billion

EXPONENTIAL GROWTH IN IOT MARKET REVENUE[8]

$656 billion
in 2015

$1.7 trillion
in 2020

China and Japan alone account for a quarter of global revenue, followed by the US

Source: APRC analysis

2 The Transparency in Cyber Risk

Transparency is key to in cyber risk management

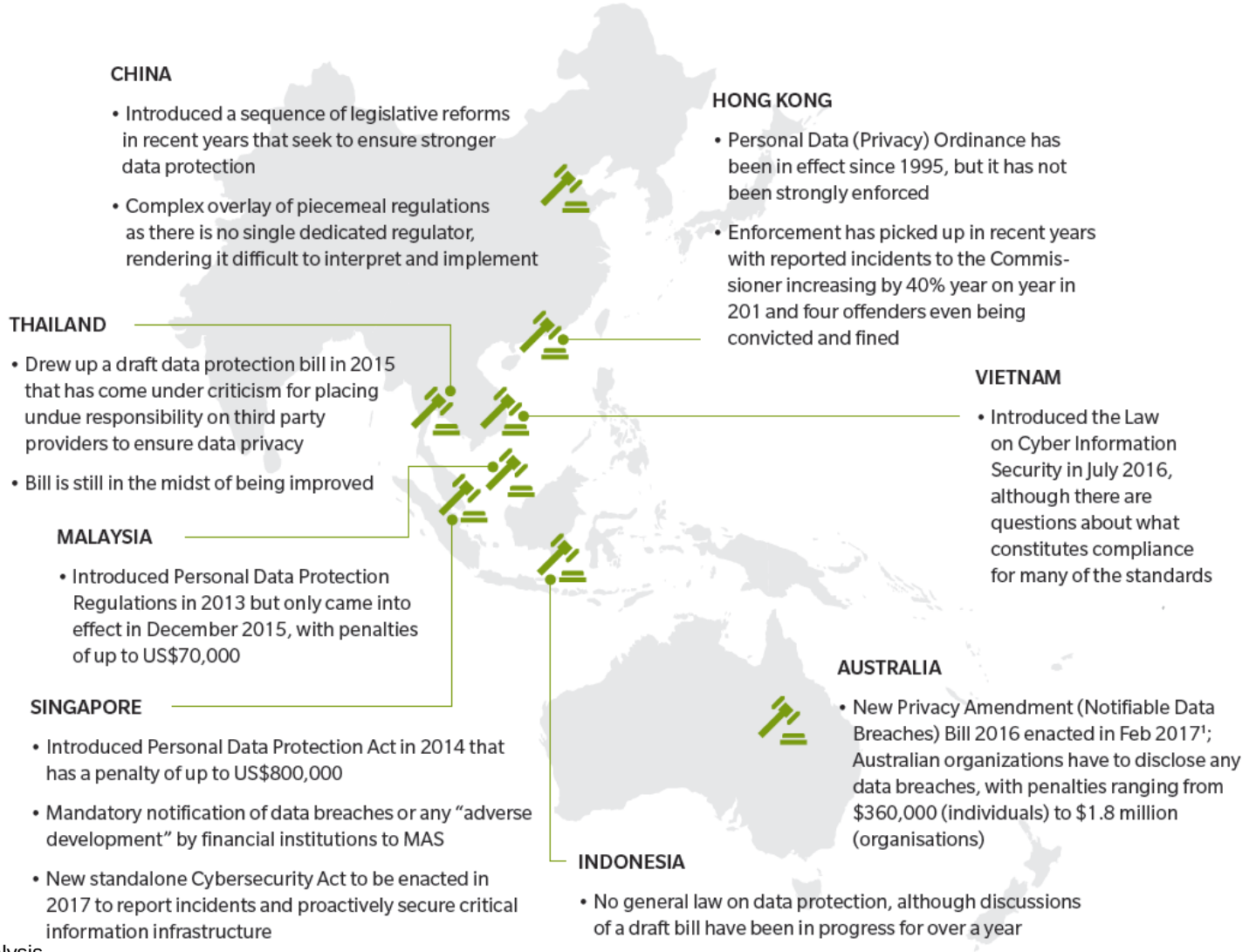
It drives awareness to catalyze actions required to overcome challenges and mitigate cyber risk

1. Increase **transparency** to stakeholders concerning cyberattacks
2. Raise stakeholder **awareness** of cyber security situation
3. Initiate stakeholder **action** to combat cyber threat
4. Overcome challenges to **mitigate** cyber risk

Source: APRC analysis

Without transparency, attempts at cyber risk mitigation by organizations and regulators would be akin to trying to hit a blind target—if at all they are even aware of one

Recent developments in data privacy legislation in APAC countries



Source: APRC analysis

3 Overcoming cybersecurity challenges

Board indifference to cyber risk continues to persist across Asia

Enterprise-wide cyber risk management not commonly accepted yet

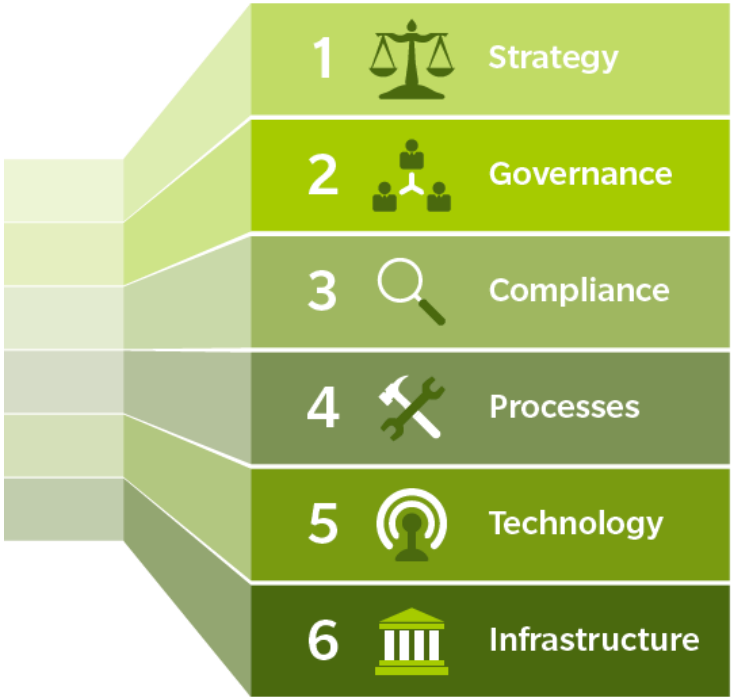
Business sentiments from the SID cybersecurity forum (July 2016)

> *The silence of many boards is worrying. More education is needed.*
>
> *– Mr. Foo Siang-tse, Managing Director, Quann*

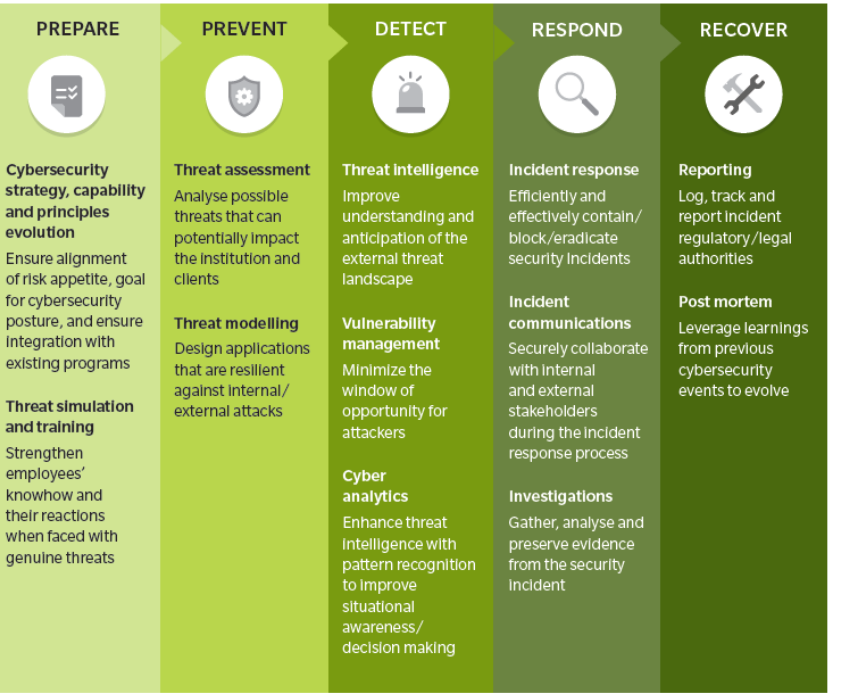
> *Cyber security is not a top priority on most board agendas. It tends to be relegated to the IT department.*
>
> *– Ms Tan Yen Yen, Regional Vice President, SAS Institute*

Robust enterprise-wide cyber risk management skills start from the Board and cybersecurity is the responsibility of all staff

From applying an enterprise-wide risk framework…



… to building cybersecurity capabilities along the "Kill Chain"



Source: APRC adaptations of Oliver Wyman analyses

Efforts for cyber risk management should occur at an enterprise level to become mainstay on the Board agenda, forming part of the strategic business plan

Cyber risk quantification justifies the level of cybersecurity investment and risk mitigation

Challenges

#1 Modelling framework and development

- Narrow definition – focusing only on direct revenue losses

#2 Data availability and reliability

- Gather and collect all relevant data:
  - Internal and external records of business
  - Operational and technical
- Scarce historical data due to the recent nature of cyber trends

#3 Decision-making

- Pricing of risk exposure and making risk-adjusted decisions difficult due to:
  - Lack of transparency
  - Incomplete information

Suggested solutions

- Scenario analysis with at least three variants:
  - Foregone revenue
  - Liability losses
  - Reputational damage
- Rely on the educated assumptions of third-party experts to support their model build
- Robust risk quantification model to assess the adequacy of their risk protection and determine the necessity for further investments

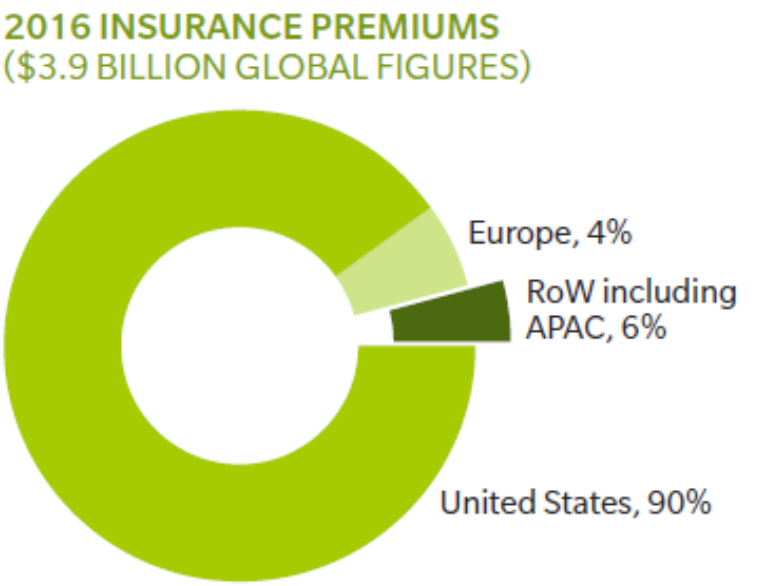
A key role of insurance is risk transfer

Since cyber risk cannot be eliminated, companies must be prepared for a cyberattack

Globally cyber insurance is gaining traction…

- Severity of cyber risk:
  - Tail risk to data, reputation, and ability to conduct business
  - Average total cost of data breach is $4 million in 2016, up 29% from 2013
- Growing cyber insurance market globally:
  - Annual gross written cyber insurance premiums grew 34% per annum to $3.9 billion in 2016, from $500 million in 2009
  - Projected strong long-term growth to reach $9 billion by 2020

… but market remains heavily skewed



Large market share primarily driven by is the mandatory breach notification laws (47 out of 50 states in the US have enacted the legislation)

[1]*Source: APRC analysis of data from MMC and Munich Re*

QUALIFICATIONS, ASSUMPTIONS AND LIMITING CONDITIONS

This report is for the exclusive use of the MMC client named herein. This report is not intended for general circulation or publication, nor is it to be reproduced, quoted or distributed for any purpose without the prior written permission of MMC. There are no third party beneficiaries with respect to this report, and MMC does not accept any liability to any third party.

Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been independently verified, unless otherwise expressly indicated. Public information and industry and statistical data are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information. The findings contained in this report may contain predictions based on current data and historical trends. Any such predictions are subject to inherent risks and uncertainties. MMC accepts no responsibility for actual results or future events.

The opinions expressed in this report are valid only for the purpose stated herein and as of the date of this report. No obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

All decisions in connection with the implementation or use of advice or recommendations contained in this report are the sole responsibility of the client. This report does not represent investment advice nor does it provide an opinion regarding the fairness of any transaction to any and all parties.

MARSH RISK CONSULTING