MARSH

ASIA PACIFIC RISK CENTER

CYBER RISK IN ASIA-PACIFIC

THE CASE FOR GREATER TRANSPARENCY

RISK IN FOCUS SERIES

- TRANSPARENCY IS THE FIRST STEP TOWARDS CYBER RISK MITIGATION
- GOVERNMENTS AND CORPORATIONS CAN ENHANCE TRANSPARENCY AND MANAGE CYBER ADVERSARIES
- TOOLS AND STRATEGIES TO BUILD CYBER RESILIENCE

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

KEY TAKEAWAYS

1. Raising the transparency level is the first step to cyber risk mitigation – it leads to higher visibility and greater awareness necessary to catalyze actions required to mitigate cyber risks.

2. Asia-Pacific (APAC) is an ideal environment for cyber criminals to thrive in due to high digital connectivity, contrasted with low cybersecurity awareness, growing cross-border data transfers and weak regulations.

3. The lack of transparency leads to an inaccurate perception that the APAC cyber threat level is lower than other regions.

4. Detailed and clear data breach notification laws, supported by enforcement, and a culture of compliance within organisations are critical to improving transparency and improved risk mitigation.

5. The global cyber insurance market is heavily skewed towards the US, driven primarily by the mandatory breach notification laws that raise the transparency and awareness levels among key stakeholders.

6. Beyond legislation, governments can further mitigate cyber risk through public-private information sharing, development of cybersecurity knowledge hubs and growing the cybersecurity talent pool.

7. Companies need to start treating cyber risk as an enterprise-wide risk by applying a comprehensive risk management framework and upgrading its capabilities along the cybersecurity "Kill Chain". The reality is that many APAC organizations lack the structure, processes or culture necessary for this.

TABLE OF CONTENTS

INTRODUCTION

Cybercrime is becoming a greater risk when doing businesses in Asia-Pacific (APAC) as compared to North America and Europe. Rapidly growing connectivity and the accelerating pace of digital transformation expose the APAC region, and make it particularly vulnerable to cyber exploitation. Evidently, according to the 2017 edition of the Global Risks Report, cyber concern around the likelihood and impact of technological threats has sharpened among business executives in APAC, and cyberattacks are ranked among the top 5 risks of doing business in the region.

The lack of transparency in the region results in weak cyber regulations and enforcements by authorities, as well as low cyber awareness and security investments among corporations.

Historically, data breach notification laws have been lacking across the region, bringing forth one key insight – governments and policy-makers have yet to recognize the importance of transparency in the battle against cyberattacks. Moreover, the lack of transparency potentially shrouds perceptions and alters behaviors of corporations, resulting in inaction or inadequate mitigation efforts. The global cyber insurance market is dominated by the US due to the mandatory breach notification laws that raise transparency and awareness levels among key stakeholders. Cyber insurance take-up rates in APAC remains negligible today.

To mitigate cyber risk, it is essential to raise the degree of cyber transparency in the region. Besides addressing the inevitable challenges related to government actions and corporate reactions to push for transparency, there must also be buy-in for comprehensive cyber risk strategies and fair collaboration among various stakeholders to build cyber resilience within the cybersecurity ecosystem.

For the purpose of this report, we use a definition of Asia-Pacific that includes East Asia, South Asia, Southeast Asia and Oceania, but excluding central Asia and the countries of the Easten Pacific (North and South America).

CYBER RISK: ASIA-PACIFIC IN NUMBERS

THE SEVERITY OF CYBERATTACKS

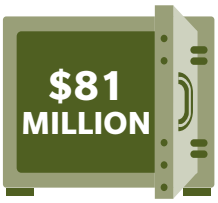
in business revenues lost to cyberattacks[1]

Ranked **5th** among **Asian** top risks[2]

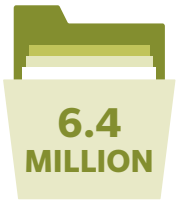
Ranked **6th** among **Global** top risks[2]

RECENT CYBERATTACKS EXAMPLES IN ASIA

personnel stolen from Singapore's defense ministry online database portal in Feb 2017[4]



stolen from cyberattack on a bank in Bangladesh in May 2016[5]



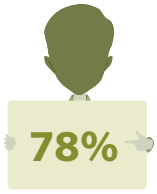
Children's data stolen in Hong Kong hacking of a digital toymaker firm in in Dec 2015[7]

Philippine government websites **simultaneously hacked** in July 2016[6]

ASIAN FIRMS LAG IN CYBERSECURITY

Asian organisations take **1.7 times** longer than the global median to **discover a breach**[8]

Asian firms spent **47%** less on information security than North American firms[9]



of Internet users in Asia have **not received any education** on cybersecurity [10]

CHALLENGES FOR FIRMS IN MANAGING CYBERSECURITY

70% of firms do not have a strong understanding of their cyber posture

of organisations found it "difficult-to-extremely-difficult" to recruit cyber talent[11]

Primary insurers are reluctant to provide single coverage above **$100 MILLION**

1 FT, 2016. Asia Hacking: Cashing in on cybercrime.
2 WEF and Marsh & McLennan Companies, 2017. The Global Risks Report 2017, 12th Edition.
3 BBC News, 2016. Asian companies have world's worst cybersecurity says study.
4 Straits Times, 2017. Personal data of 850 national servicemen and Mindef staff stolen in targeted cyberattack.
5 Reuters, 2016. Bangladesh Bank official's computer was hacked to carry out $81 million heist.
6 The Philippine Star, 2016. 68 government websites attacked.
7 CNBC, 2015. Vtech hack: Data of 6.4M kids exposed.
8 Mandiant, 2017. M-Trends 2017: A view from the front line.
9 Gartner, 2015. Information Security Spending Update.
10 ESET, 2015. EEST Asia Cyber-Savviness Report 2015.
11 Mercer, 2015. Human Capital Challenges in a High-Risk Environment: 2015 Cybersecurity Talent Spot Poll.

PART 1: GLOBAL TRENDS IN CYBER RISK

Only in the last decade has cyber risk emerged as a real threat as the world becomes increasingly digitized. Cyberattacks are known to be low-cost yet capable of severe damages, while cyber adversaries are not limited by geographical boundaries. With its ever evolving nature, cyber risk has grown pervasive and dangerous, rendering it hard to combat.

Today, cyber risk is entrenched in the operations of organizations across all industries and geographies, making them susceptible to cyberattacks regardless of their cybersecurity measures. Losses from cyberattacks can also be significant – including compensations to impacted customers, business interruptions, or reputational damage.

Every year, the World Economic Forum (WEF) partners with Marsh & McLennan Companies to prepare one of its flagship publications, the Global Risks Report. In the 2017 edition, cyberattacks are ranked as the 6th most likely global risk over the next decade[2]. The scope, scale and impact of cyberattacks have grown rapidly as cyberattacks were not considered a top 10 global risk till 2012.

*Global cost of data breaches estimated to reach **$2.1 trillion**[12] by 2019*

Alarmed by the growing cyber risk trends, countries in the West have begun taking measures to mitigate the threat. In April 2016, Europe adopted the General Data Protection Regulation (GDPR), which will take effect in 2018. Hailed as a watershed, the GDPR mandates that every company doing business in Europe and handling personal data relating to EU-based citizens to disclose data breaches to authorities and the public, where necessary. More importantly, failure to do so warrants a financial penalty up to 4 percent of total revenues.[13]

Governments are investing in cyber research, developing knowledge centers that provide guidance on cyber practices and technical issues, and facilitating knowledge exchange between industries.

The private sector has also seen growing awareness. A 2016 study on cybersecurity practices in Europe found that the number of companies that list cyber as a top-five concern has doubled in the last year while companies that did not mention cyber as a concern dropped from 25 to 10 percent.[13] Boardrooms are also maturing in their cyber risk perception and managing cyber risk at the enterprise level.

While global awareness of growing cyber threat is rising, decisive corporate actions are still lacking. Of the 30 percent of companies[13] that reported an understanding of their cybersecurity plans, many have yet to take concrete actions to institutionalize cyber risk management plans into their longer-term business strategies.[14]

12 Juniper Research, 2015. The Future of Cybercrime & Security: Financial & Corporate Threats & Mitigation 2015-2020.
13 MMC Global Risk Center, 2016. MMC Cyber Handbook 2016/17.
14 Swiss Re Institute, 2017. Sigma Series – Cyber: Getting to grips with a complex risk.

PART 2: ASIA-PACIFIC – A PERFECT CYBER STORM?

Asia is 80 percent more likely to be targeted by hackers than other parts of the world.[3] The number of high profile cyber incidents has risen in recent years, although we assert that the public sees only a sliver of the real impacts of such incidents.

A HIGHER THREAT POTENTIAL

SPEED OF DIGITAL TRANSFORMATION

MORE INTERNET USERS GLOBALLY[16]

3.7 billion
in 2016

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

GREATER INTERCONNECTIVITY AMONG 4G MOBILE DEVICES[17]

1 billion
(connections) in 2015

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

HIGHER MOBILE NETWORK TRAFFIC[18]

7EB/mth
in 2016

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

ASIA PACIFIC LEADS INTERNET-of-THINGS (IoT) MARKET

TECHNOLOGY ADOPTION PIONEERS[19]
Japan and South Korea pioneered the adoption of IoT and machine-to-machine technology

TOP BROADBAND (INTERNET) SPEED

27 Mbps

19.5 Mbps[20, 21]

compared to global average of **5.6 Mbps**

GLOBAL IoT CONNECTIVITY[22]

4.9 billion
(units) in 2015

25 billion
in 2020; with APAC contributing 8.6 billion

EXPONENTIAL GROWTH IN IoT MARKET REVENUE[23]

$656 billion
in 2015

$1.7 trillion
in 2020

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

Reasons for the relatively higher cyber threat potential in APAC are twofold: the growing speed and scope of digital transformation, and the expanding sources of vulnerability stemming from increasing IoT connectivity.

15 Internet World Stats, 2017. World Internet Users and 2017 Population Stats.
16 eMarketer, 2016. 4G Mobile Connections and Penetration Worldwide, by Region, 2015 & 2020.
17 Cisco, 2017. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper.
18 Tech in Asia, 2015. Three factors driving IoT in Southeast Asia.
19 Akamai, 2016. State of the Internet Report.
20 Tech in Asia, 2016. Asia's mobile and broadband internet speeds, in one infographic.
21 First Post, 2015. APAC becomes IoT champion: 8.6 billion connected things, $583 billion market by 2020.
22 WSJ, 2015. Internet-of-Things Market to Reach $1.7 trillion by 2020: IDC.

ACCELERATING DIGITAL TRANSFORMATION IN APAC

Digital transformation – the connection of individuals, companies, and countries to the Internet – has emerged among the most transformative means to ignite sustainable growth. This is most evident in APAC where strong economic growth in recent years has been powered by the rapid adoption of Internet and mobile technologies.

Across the region, a few emerging economies have accelerated their digital transformation so rapidly that they have bypassed certain various stages of technology development – just over the past few years many people across several Asian countries have leapfrogged from not having any Internet access at homes to owning multiple mobile devices and accessing the Internet. For example, estimates from The World Bank indicate 22 percent of Myanmar is now online, compared to less than 2 percent in 2013, opening abundant opportunities for the domestic consumer market.

In Indonesia, meanwhile, mobile device subscription rates were estimated to be higher than the rest of Asia in 2015 (132 percent vs 104 percent). The high subscription rate was one key driving force propelling the domestic mobile-money industry – annual e-money transaction values in Indonesia grew almost to Rp5.2 trillion ($409 million) in 2015 from Rp520 billion ($54.7 million) in 2009.[23]

Unfortunately, there remains a huge gap in cybercrime legislations in these countries – the lack of awareness and knowledge of basic security makes most online transactions highly susceptible to digital theft. While the breakneck speed of digital transformation is generally good news, safeguards must be in place alongside to protect users and sustain the burgeoning digital business.

EXPANDING SOURCES OF VULNERABILITY

The rapid spread of internet-enabled devices – IoT – enables new and more efficient modes of communications and information sharing. Asia-Pacific, in various aspects, leads in the IoT technology: South Korea, Australia, and Japan are among the top five countries, reaping the most benefits from IoTs, according to the 2016 International Data Corporation's (IDC) "*Internet-of-Things Index*".[24]

Over time, IoT technology will create and add a significant fleet of digitally-connected devices, most of them originating from APAC – China, Japan, and South Korea are constantly looking to "smartify" all possible consumer electronics, for example.

However, higher interconnectivity through the plethora of IoT devices "opened up new means of attack", according to William H. Sato, Special Advisor to the Cabinet Office, Government of Japan.[25] In October 2016, one of Singapore's main broadband networks suffered a severe Distributed Denial of Services (DDoS) attack, causing two waves of internet-surfing disruptions over one weekend. Investigations revealed the security vulnerability was exposed through compromised IoT devices, such as customer-owned webcams and routers.[26] Such smaller personal IoT devices are increasingly targeted since they potentially provide a backdoor into more robust security systems.

23 Antara News, 2016. E-money transactions reach Rp5.2 trillion: Bank Indonesia.

24 IDC, 2016. IDC Launches Updated G20 Internet of Things Development Opportunity Index Ranking.

25 BRINK Asia, 2017. Moving beyond fear, uncertainty, and doubt on cyberattacks.

26 Channel News Asia, 2016. DDoS attack on StarHub first of its kind on Singapore's Telco.

WEAKER CYBER RISK MITIGATION EFFORTS

Despite the ever-present and ever-growing cyber threat potential in APAC, companies in the region appear less prepared. A lack of transparency has resulted in low levels of awareness and insufficient cybersecurity investments.

LOW AWARENESS

A survey conducted by ESET Asia in 2015 revealed that 78 percent of Internet users in Southeast Asia have not received any formal education on cybersecurity,[10] highlighting that most people in the region are oblivious to their cyber vulnerabilities.

The lack of disclosure regulation has also created the perception that cyberattacks in the region are relatively lower than those reported in the US or Europe, even though Asian businesses are significantly more likely to be targeted.

LOW INVESTMENTS

The low level of awareness in general leads to an underinvestment of time, finances, and resources in the technologies and processes needed to combat cyber adversaries.

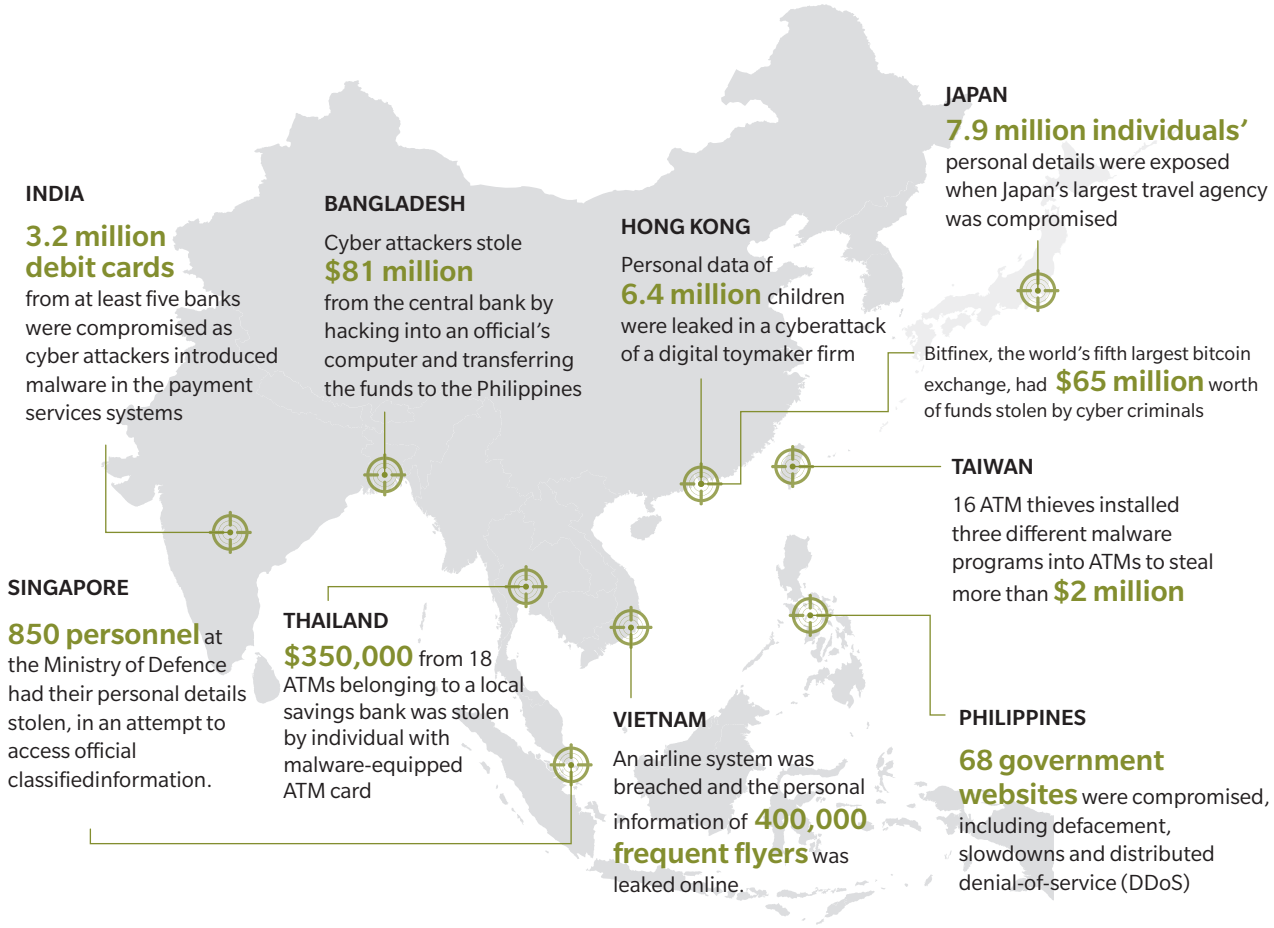
For example, a 2016 Beazley survey[27] found 80 percent of the surveyed small-medium enterprises (SMEs) in Singapore used anti-virus software as their main cyber risk management tool, while only 8 percent allocated more than $50,000 to their cybersecurity budgets. Furthermore, APAC firms on average spent 47 percent less on information security than North American firms in 2015.[9]

27 Beazley, 2016. Cybersecurity: A Growing Concern for Singapore SMEs.

ASIA-PACIFIC – A PRIME TARGET FOR CYBERCRIME

The need to combat cyber threat has never been more urgent in the APAC region, and major industries in the region (construction and engineering, financial, high tech and electronics, for example) are especially susceptible to the threats.[8] A series of recent, high-profile cyberattacks that touched multiple countries and industries across the region have brought the issue to the fore (Exhibit 1).

Exhibit 1: Cyberattacks in APAC – Tip of the iceberg?



Yet, these incidents represent only a handful of all attacks. LogRhythm, a security intelligence company, estimated up to 90 percent of APAC companies came under some form of cyberattack in 2016. A survey by Grant Thornton revealed that business revenues lost to cyberattacks in APAC amounted to $81.3 billion in 2015, exceeding those in North America and Europe by approximately $20 billion each.[1]

What is worrying is that this is likely only the tip of the iceberg. Cheah Wei Ying, an expert on non-financial risk at Oliver Wyman believes that "the majority of cyberattacks in the region usually go unreported as companies are neither incentivized nor required to do so. This lack of transparency underpins APAC's susceptibility to cyberattacks".

Apart from selected countries (i.e. Japan, South Korea) and industries (i.e. financial services in Singapore), APAC still lags the West in terms of cyber transparency. Organizations are able to conceal data compromises from regulators and their stakeholders, dulling the true impacts of cyberattacks and impeding the threat awareness required to act against cyber criminals.

In the region's battle against cybercrime, the most critical issue is raising the level of transparency.

PART 3: THE NEED FOR TRANSPARENCY

We define, for purposes of this report, transparency as the disclosure of the scale and nature of cyberattack to key stakeholders (for example, Board members, affected clients and suppliers, and regulators).

Within the cyber risk context, transparency allows key stakeholders to easily observe and make visible the true state of cybersecurity, and increase their awareness of existing cyber adversaries. Consequently, they can undertake targeted actions to improve detection capabilities and combat the threat.

Thus, transparency is critical as the first step in risk mitigation, driving awareness necessary to catalyze actions required to overcome challenges and mitigate cyber risk (Exhibit 2). Without that, attempts at cyber risk mitigation by organizations and regulators would be akin to trying to hit a target blind – if they are even aware of one.

Exhibit 2: The role of transparency in mitigating cyber risk

TRANSPARENCY TRENDS IN ASIA-PACIFIC

The lack of transparency in APAC has led to an inaccurate perception that cyber threat is lower here than elsewhere, influencing the attitude of regulators by eroding the urgency for cybersecurity. Consequently, nations and organizations become systematically underprepared, exposing a soft underbelly that cyber attackers have repeatedly exploited.

The degree to which the region lags behind is highlighted in research findings by Mandiant, which found the median time for Asian organizations between a breach and its discovery almost doubled the global average (that is, 172 versus 99 days).[3]

Underpinning the region's transparency issue is its historical lack of data breach notification laws. These laws typically require companies that are compromised to inform regulators and affected stakeholders, and to take steps to remediate – failure to do so would result in a heavy penalty. Although it breaks the opacity that most organizations would rather prefer, these legislations keep companies accountable to their stakeholders by protecting the reputation and minimizing losses at source.

Nonetheless, with regulators unable to keep up with the speed of digital transformation, APAC governments have been slow in implementing these laws. This is contrary to the West, where progress has been incremental, giving regulators time to adapt, assess, and implement necessary safeguards.

EVOLVING BUT STILL INADEQUATE LEGISLATION

High profile cyberattacks in recent years have caught the attention of APAC lawmakers: Singapore, Malaysia, Vietnam, and China have either introduced or updated their data privacy laws, the first layer of cybersecurity, to ensure better management, security, and control of data.[28] Others, such as Thailand and Indonesia, lag a little but have also began the legislative process.

However, many APAC countries still lack the notification clauses for data breach, with the exception of Japan, Australia, South Korea, and the Philippines.[29] Moreover, countries such as Singapore require breach notifications only from financial institutions, as they are imposed by the Monetary Authority of Singapore (MAS), the industry-specific regulator.[30] Lastly, some companies may only be required to disclose breaches to regulators and not to other stakeholders (i.e. customers and shareholders).

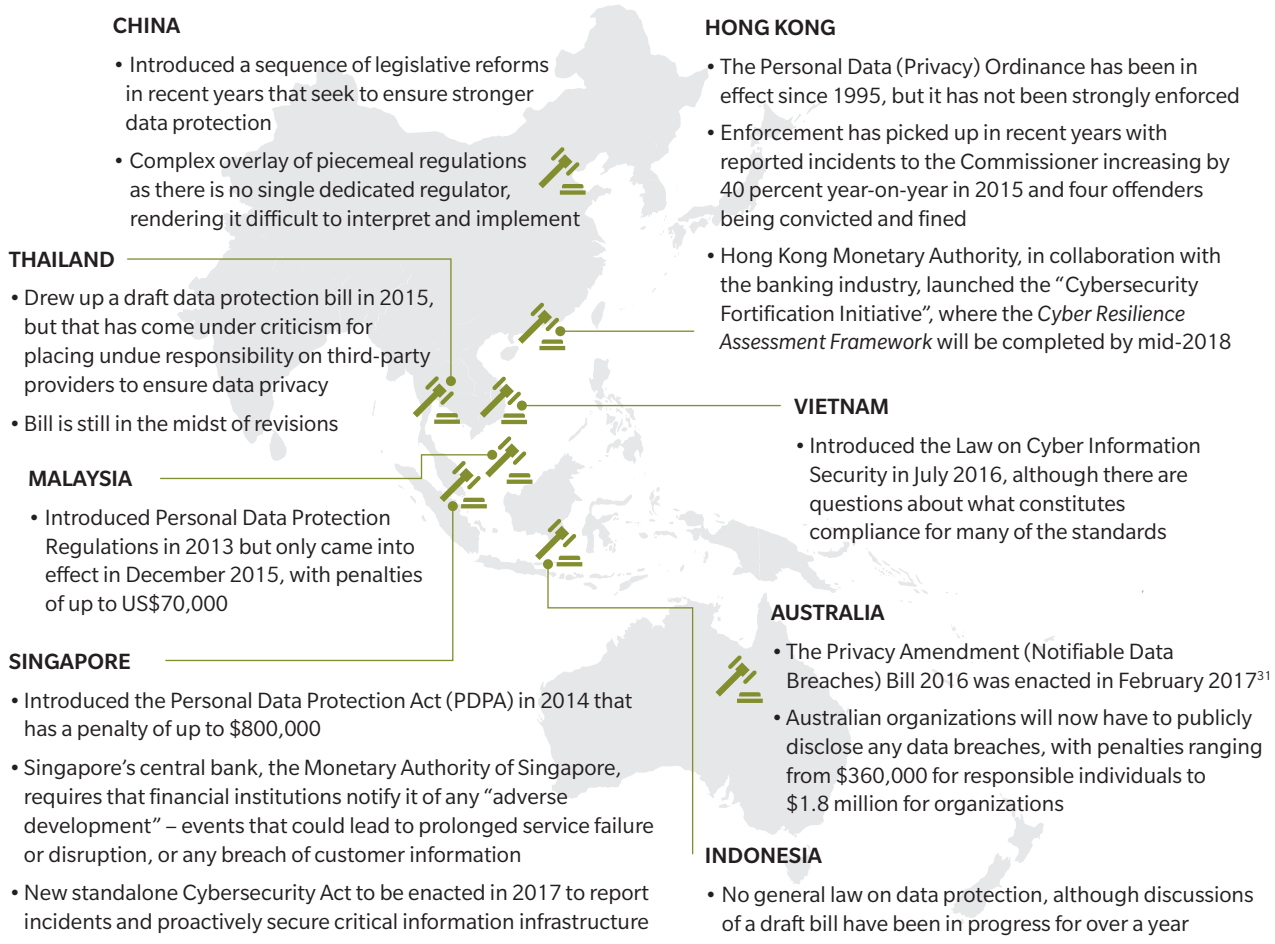
The progress towards transparency is thus piecemeal across all levels. The lack of convergence on breach notification regulations in the region suggests that governments have yet to recognize the key role that transparency plays in the fight against cyber risk – a perception that needs to change urgently.

28 Hogan Lovells, 2016. Cybersecurity Regulation in Asia: The Tightening Lines of Defense.

29 Bloomberg BNA, 2015. Privacy and Security Law Report.

30 Monetary Authority of Singapore, 2014. Technology Risk Management Notice and Guidelines.

Exhibit 3: Developments in data privacy and breach discolosure regulations



CHINA

- Introduced a sequence of legislative reforms in recent years that seek to ensure stronger data protection
- Complex overlay of piecemeal regulations as there is no single dedicated regulator, rendering it difficult to interpret and implement

HONG KONG

- The Personal Data (Privacy) Ordinance has been in effect since 1995, but it has not been strongly enforced
- Enforcement has picked up in recent years with reported incidents to the Commissioner increasing by 40 percent year-on-year in 2015 and four offenders being convicted and fined
- Hong Kong Monetary Authority, in collaboration with the banking industry, launched the "Cybersecurity Fortification Initiative", where the *Cyber Resilience Assessment Framework* will be completed by mid-2018

THAILAND

- Drew up a draft data protection bill in 2015, but that has come under criticism for placing undue responsibility on third-party providers to ensure data privacy
- Bill is still in the midst of revisions

VIETNAM

- Introduced the Law on Cyber Information Security in July 2016, although there are questions about what constitutes compliance for many of the standards

MALAYSIA

- Introduced Personal Data Protection Regulations in 2013 but only came into effect in December 2015, with penalties of up to US$70,000

AUSTRALIA

- The Privacy Amendment (Notifiable Data Breaches) Bill 2016 was enacted in February 2017[31]
- Australian organizations will now have to publicly disclose any data breaches, with penalties ranging from $360,000 for responsible individuals to $1.8 million for organizations

SINGAPORE

- Introduced the Personal Data Protection Act (PDPA) in 2014 that has a penalty of up to $800,000
- Singapore's central bank, the Monetary Authority of Singapore, requires that financial institutions notify it of any "adverse development" – events that could lead to prolonged service failure or disruption, or any breach of customer information
- New standalone Cybersecurity Act to be enacted in 2017 to report incidents and proactively secure critical information infrastructure

INDONESIA

- No general law on data protection, although discussions of a draft bill have been in progress for over a year

31 Office of the Australian Information Commissioner, 2017. Mandatory data breach notification.

CHALLENGES REMAIN

Other outstanding issues remain to be resolved, such as misalignment of regulations and perceptions, enforcement, and the culture of compliance within organizations.

First, regulations imposed may not be aligned to the general opinion of organizations. A 2014 survey of industry leaders conducted by the WEF found 56 percent of respondents felt that cybersecurity regulations did not make their organizations any more secure, with a third of those believing that it actually made them less secure by requiring actions that take resources away from other actions of higher priority.[32] Given that many regulations in APAC have only been recently implemented, it is still early days to judge their efficacy.

Enforcement is another issue of concern. While some APAC countries have begun to display willingness in enforcing data privacy laws (for example, Australia, Japan, South Korea), there are still a handful taking a more passive approach (such as Malaysia, the Philippines).

Among countries that promote enforcement, the approaches and effectiveness vary widely, resulting in different levels of adherence. For example, South Korea is quick to impose fines while Japan and Hong Kong prefer minimal state intervention, choosing instead to encourage dispute resolution between affected parties for small incidents. Taiwan's enforcement is carried out by industry-specific regulators, leading to inconsistent standards nationwide, while Singapore seeks greater collaboration with industry to promote compliance.[30]

Finally, while there is a strong onus on the government to regulate corporate behavior, success is heavily dependent on the organizations' readiness to adhere to regulations. The reality is that many APAC organizations lack the structure, processes or culture necessary for this. Companies will require support, guidance and time to gather the ingredients necessary to meet regulators' expectations.

Considering the current state of affairs in APAC and the factors listed above, it is evident that the region still has some way to go before it is able to successfully implement, enforce and encourage compliance with data breach notification regulations. Nevertheless, there should be a continued emphasis on enacting this fundamental law to achieve transparency, which is necessary to drive the awareness and action for cyber risk mitigation.

32 World Economic Forum, 2014. Risk and Responsibility in a Hyperconnected World.

PART 4: RAISING AWARENESS AMONG KEY STAKEHOLDERS

Raising the level of transparency is intended to raise the awareness of key stakeholders who can effect change in the fight against cyberattacks. On this cyber battlefield, the three stakeholders that hold the key to overcoming cyber adversaries are the government, the organizations, and the individual (Exhibit 4).

Overcoming the cyber adversary requires awareness and action from all three parties. The next section discusses different actions that these stakeholders can take to mitigate cyber risk, particularly governments and corporations, as these will form the focus of the remaining sections.

Exhibit 4: Every stakeholder has a role to play against cybercrime

STAKEHOLDER	GOVERNMENT	ORGANISATION	INDIVIDUAL
WHY IS THIS STAKEHOLDER IMPORTANT?	**Change organisational behavior** – compel organizations to behave in a cyber-resilient manner that they are otherwise not incentivised to do **Sits across organisations** – leverage the lessons from a few organizations to benefit many **Influence national institutions** – exert influence on national institutions (for example, education, media) that play a key role in resolving cyber risk issues	**Valuable target** – organisations contain treasure troves of customer information **First line of defense** – build a strong first line of defense at the epicenter of cyberattacks	**The weakest link** – a 2014 study by IBM found that human error was a contributing factor in more than 95% of cyberattacks. Increasing a company's or nation's cyber resiliency requires greater awareness from its individuals **Keep companies accountable** – customers and shareholders can apply pressure and keep companies accountable, incentivizing them to make cyber risk a boardroom issue
HOW TO RAISE AWARENESS IN STAKEHOLDER?	**"Company to government" transparency** afforded by comprehensive and enforceable data breach notification regulations	**Internal transparency** built on processes for upward breach notification and supported by an open culture **"Government to company" transparency** through public-private partnerships and information sharing **"Company to company" transparency** through private partnerships	**"Company to individual" transparency** through trainings and updates on cyber weaknesses and breaches **"Government to individual" transparency** through national campaigns and the media

PART 5: GOVERNMENT ACTIONS TO MITIGATE THE RISK

The ultimate purpose of raising the level of transparency and awareness among different stakeholders is to ensure they take actions to mitigate the cyber threat. In the fight against cybercrime, the government is more than just a regulator, holding the authority to create and shape a more conducive landscape to mitigate cyber risks. Another key element is the establishment and promotion of cybersecurity standards or framework.

For example, the National Institute of Standards and Technology (NIST) Cybersecurity Framework is widely known as processing the best practice for computer security, which was first directed by a presidential executive order in 2014 intended to help organizations manage cybersecurity risk in critical infrastructure in the US. Another example is the Australian Cybercrime Online Reporting Network (ACRON), a national online system that consolidates cybercrime incidents reported securely by the public.

Here, we discuss three main ideas likely to deliver significant risk mitigation impacts: public-private information sharing, the development of cybersecurity knowledge hubs, and growing the cybersecurity talent pool. While most APAC governments have yet to undertake these initiatives, there have been plans for consideration by some forwardlooking ones.

PUBLIC-PRIVATE INFORMATION SHARING

A useful defense tool against cyberattacks, both public and private sectors can consolidate important information to obtain a fuller view of the cyber risk in the fight against cybercrime. This was echoed by **Peter Beshar**, Executive Vice President and General Counsel of Marsh & McLennan Companies, who spoke at the 2016 Presidential Commission on Enhancing National Cybersecurity in New York.

"The vision articulated in the Cybersecurity Act of 2015 to create a real-time information sharing platform of cyber threat indicators needs to be made operational."[33]

With increasing connectivity and digital dependency, especially in financial services sector, sharing of timely and actionable cyber information among institutions and regulators is the first-step to build cyber resilience within the industry.

This is evident in the recently established Asia-Pacific Regional Intelligence and Analysis Centre (the Centre),[34] a partnership between the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the MAS. The Centre is expected to commence operations by mid-2017, intending to coincide with the new Cybersecurity Act in Singapore.[35]

33 MMC, 2016. Testimony of Peter J. Beshar – Before the Presidential Commission on Enhancing National Cybersecurity, 16 May 2016.

34 Monetary Authority of Singapore, 2016. FA-ISAC and MAS establish APAC Intelligent Center.

35 Business Times, 2016. Singapore to introduce Cybersecurity Act and boost cybersecurity expenditure.

The key objective of the Centre is the reciprocal sharing of cyber threat indicators between the public and private sectors, as well as reinforcing inter-governmental collaborations, which are expected to strengthen the APAC cybersecurity ecosystem.

However, some governments in APAC are cautious about sharing information and hence remain one step behind their cyber adversaries. Vietnam, for example, retains a paternalistic stance towards its citizens, most recently embodied by its new cybersecurity laws that greatly favor centralized cybersecurity over the right to privacy by its citizens. This top-down approach is common among many Asian governments, holding the perception that their people must be managed rather than partnered with.

DEVELOPING CYBERSECURITY KNOWLEDGE HUBS

Building a cyber-resilient organization requires experience and technical expertise, both of which are in short supply in the region. Cybersecurity hubs can act as repositories for cutting edge innovation, technology and practices that can help companies narrow the knowledge gap necessary to build effective cyber defense.

One positive example is that of the Australian government, which has rolled out a couple of initiatives on cybersecurity and established numerous knowledge and collaboration hubs for this purpose.

The Australian Signals Directorate (ASD) Information Security Hub[36] opened in 2012 to increase engagement with schools through outreach programs such as internships and work experience schemes for tertiary students to better understand cybersecurity in the digital industries. The hub also conducts key research on the latest advancements in information security, and on new information and communications technology (ICT) applications.

Another recent initiative is the A$30 million investment of a national cybersecurity mega-hub, Data61, which opened in Melbourne in 2016. The digital research arm of the Commonwealth Scientific and Industrial Research Organisation (CSIRO) shares its physical grounds with:

- Oxford University's first international office, the *Global Cybersecurity Capacity Centre*, and
- Victoria's newly set up *Oceania Cybersecurity Center* (affiliated with eight local universities, the Defense Science Institute, and various private sector organizations like Australian Post and Optus, to name a few)

36 Australian Government Department of Defence, 2017. ASD Information Security Hub

GROWING THE CYBERSECURITY TALENT POOL

Lastly, governments would do well to focus on increasing the supply of home-grown cybersecurity professionals. A global poll by Mercer revealed that 74 percent of organizations found it "difficult-to-extremely-difficult" to recruit cyber talent,[12] while Forbes noted that the world had a cyber-professional shortage of one million in 2016 and the shortage is expected to grow to six million by 2019.[37]

Kate Bravery, Partner and Global Practices Leader in Mercer Hong Kong, points out that

"In Asia, 42 percent of HR professionals anticipate an under-supply of cybersecurity talents in their IT/Technology function, and this is even higher in Japan (48 percent) and China (56 percent)."

Recent in-house analysis conducted by Mercer revealed the home-grown inadequacy in terms of the number of cybersecurity-experts based in Asia, since most organizations have their headquarters – and most cyber experts – based outside Asia. Nonetheless, cybersecurity jobs are growing in prevalence across the region. For example, in Japan, jobs in e-commerce security filled by locals grew more than three-fold between 2014 and 2016, while cybersecurity jobs in the internet and e-commerce industry in China grew by more than 100 percent over the same period.

The onus is on the governments to bridge this talent gap, which can be achieved by establishing a national cyber talent mandate. In Singapore, besides offering cybersecurity specializations to university course catalogues and providing cybersecurity diploma courses, all five polytechnics and the Singapore FinTech Association have signed a Memorandum of Understanding[38] to develop a strong cybersecurity talent pool in preparation of the increasing manpower demand. Additionally, Singapore's National Cybersecurity Master Plan 2018 includes further initiatives to grow the pool of cyber-trained professionals.[39]

Although it will take years before the fruits of these programs are seen, Singapore appears well-positioned to bridge the talent gap in the future. Other APAC countries will similarly benefit from following Singapore's lead in increasing their cybersecurity talent pool.

For instance, in India, the Modi government in partnership with Google through the Skill India program will train almost two million Android developers over three years, making the country the world's largest developer base by 2018.[40] Key infrastructures, expertise, and talent transfer available on-site put in place ready ingredients for India to further train a cyber-resilient talent pool of app developers. By writing more secure codes, enhancing security architects in the coding process and investing in tools for secure development from the beginning, there is less scope for vulnerabilities to be exploited towards the end of the processes.

37 Forbes, 2016. One Million Cybersecurity Job Openings In 2016.

38 Channel News Asia, 2017. Polytechnics, fintech association sign MOU to better support students.

39 GovTech Singapore, 2013. Singapore Continues to Enhance Cybersecurity with a Five-Year National Cybersecurity Masterplan 2018.

40 Forbes, 2016. Here's why Google is launching an Android training program in India.

MOVING ASEAN TOWARDS A RESILIENT CYBERSECURITY REGIME

It is in the common interest of ASEAN members to achieve a more resilient architecture for ASEAN-wide cybersecurity to ensure sustainable regional economic growth and trade competitiveness. In a white paper[41] published in 2013 to discuss cybersecurity in ASEAN, the S. Rajaratnam School of International Studies (RSIS) identified vulnerabilities where security and skills gaps could exist in the face of a serious cross-border cyber threat. The following highlights the key measures proposed as part of the comprehensive and multi-pronged framework in creating a resilient regional cybersecurity regime:

Recommendations for future developments in ASEAN

1	**Permanent coordinating mechanism**	• Functional coordination by committee • Information sharing, exchange policy experiences, coordinate security exercises
2	**Develop ASEAN-CERT***	• Facilitate region-wide coordination and cooperation • Enhance information exchange • Provide real time responses to cyber-attacks
3	**Defend watering hole attack†**	• Strengthen cyber security resilience of ASEAN Secretariat and related websites • Enhance staff knowledge on cyber security
4	**Training and capacity building**	• High quality ICT infrastructure • Skilled talent • Technology innovation
5	**Cyber-secured economic zone**	• Secure supply chain (from design to delivery) • Align with international cyber-secured security standards
6	**Citizen engagement**	• Public awareness • Citizen buy-in • Public-private cooperation
7	**Transboundary coordination and law enforcement**	• ASEAN master plan of security connectivity • Cyber defense unit within military structure
8	**Responsible state behaviors consensus**	• Advancing norms of responsible behavior • Applicability of international laws for cyber capabilities and techniques

* A computer emergency response team (CERT) is an expert group that handles computer security incidents.

† Watering hole attacks are a variant of pivot attacks, in which an attacker is able to pivot from one system (the initial victim usually with weaker security) to another system (the intended target typically with more robust security).

41 RSIS, 2013. Regional Cybersecurity: Moving towards a resilient ASEAN Cybersecurity Regime.

PART 6: CORPORATE ACTIONS FOR MANAGING CYBER RISKS

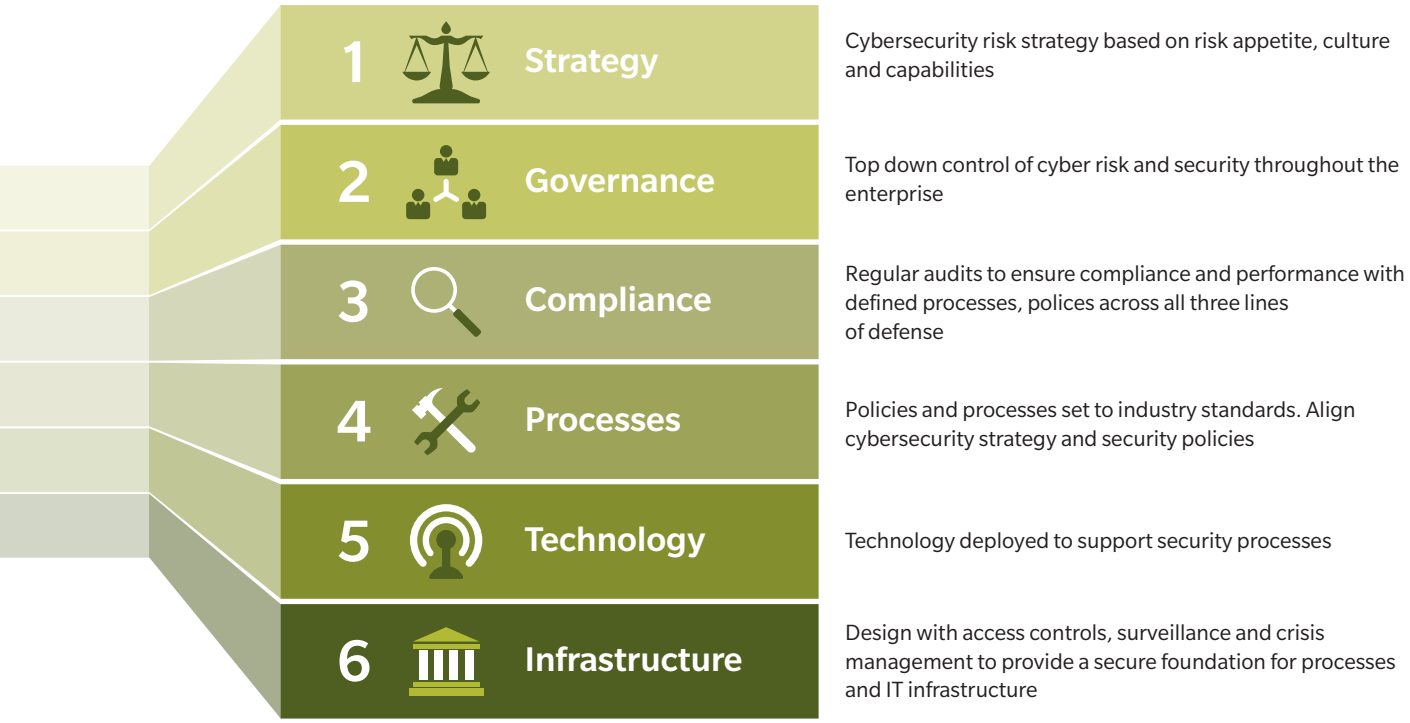
ENTERPRISE-WIDE CYBER RISK MANAGEMENT

A mindset shift is critical to catalyze a positive change in the cyber risk management strategy. Companies need to start treating cyber risk as an enterprise-wide risk, instead of leaving it solely to the IT department management.

While the IT department's mandate is to secure technological vulnerabilities, it only offers a myopic vision of cybersecurity. Beyond technology, cyber risk also represents weaknesses in the people, processes, controls and operations–components that span across the entire organization.

Robust cyber risk management skills begin with leadership from the Board and recognizing that cybersecurity is the responsibility of all staff.

Exhibit 5: Enterprise-wide cybersecurity governance begins with the Board

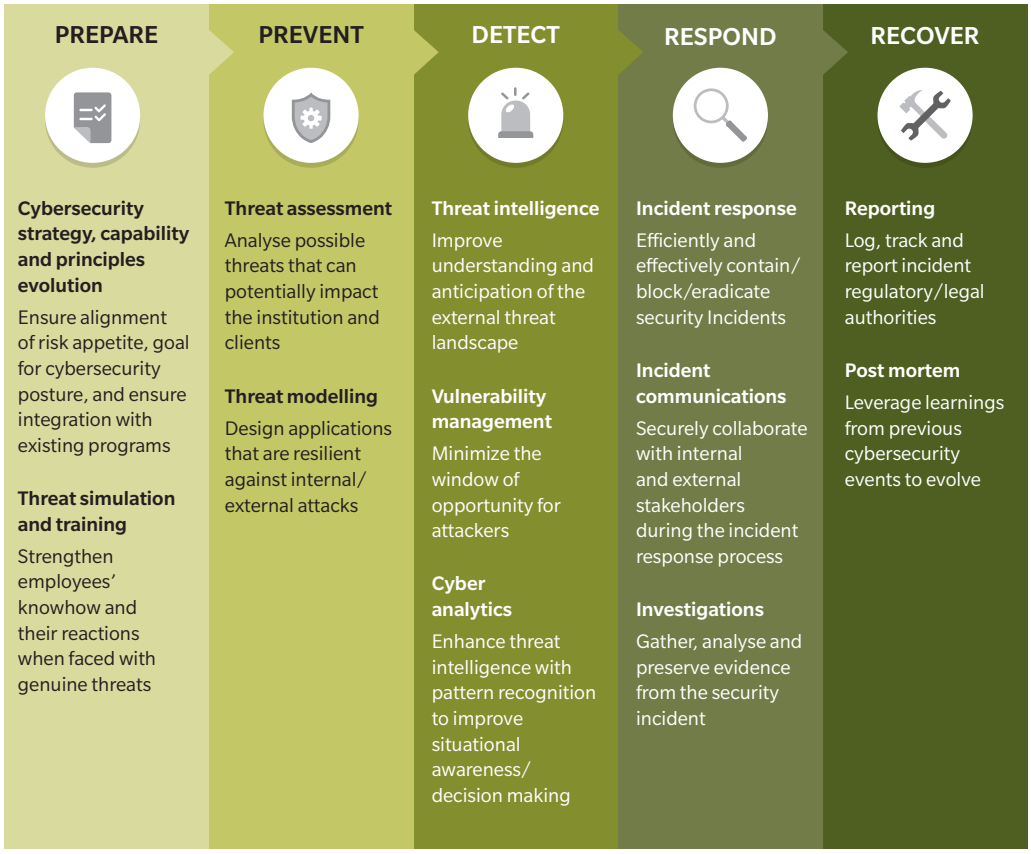


Oliver Wyman has established a cybersecurity governance framework (Exhibit 5) that establishes how companies should set themselves up to manage cyber risk at an enterprise level.

The implementation of the framework should involve everyone in the company—bearing in mind that cyber risk is not just an IT issue, but an enterprise problem. The elevation of cyber risk's importance and the expansion of its scope will equip organizations with the governance, processes and supporting infrastructure necessary for cyber-resiliency.

Having put in place a clear structure, a key next step involves building capabilities. Oliver Wyman uses a "kill chain" model to help organizations understand the five different phases through which companies can mitigate the impact of cyberattacks (Exhibit 6).

Exhibit 6: Cyber Security and the "Kill Chain"



From applying a risk framework to building capabilities along the "Kill Chain", it is imperative that the effort for cyber risk management occurs at an enterprise level and hence, becomes a mainstay on any board's agenda.

This approach is not as prevalent in APAC countries, although it has become a hot topic of discussion in more progressive economies. Singapore, in particular, is one such example. This is best encapsulated by a quote from Mr David Koh, Chief Executive of the Cybersecurity Agency of Singapore, at the Singapore Institute of Directors' (SID) Conference 2016[42]:

"The reality is that these are decisions that are core to your business, and they need to be made at the highest level, not just from within your IT department. These discussions on cybersecurity issues should be elevated from the backroom to the boardroom."

42 Singapore Institute of Directors, 2016. SID Directors' Bulletin, Quarter 4, 2016.

This sentiment was often repeated at the SID conference , indicating general acknowledgement of the need for board level involvement in dealing with cybersecurity. However, what is actually done is less ideal. Another cybersecurity forum held in July 2016 by SID[42] revealed the reality behind the words at the conference.

"The silence of many boards is worrying. More education is needed."

Mr. Foo Siang-tse,
Managing Director, Quann

"Cybersecurity is not a top priority on most board agendas. It tend to be relegated to the IT department. Instead, the board should ask for and review the cybersecurity plan."

Ms. Tan Yen Yen,
Regional Vice President, SAS Institute

Unfortunately, board indifference to cyber risk continues to persist even in Singapore, which is considered to be one of the most forward-thinking nations with regards to cybersecurity. The situation is similar or worse in other APAC countries, where the need for enterprise-wide cyber risk management is not commonly accepted.

OVERCOMING PRACTICAL CHALLENGES

Moving towards an enterprise-wide cyber risk management approach is a large and complex undertaking for any organization. This section highlights key challenges management must consider when addressing cyber risk, as well as potential solutions to overcome them.

QUANTIFYING CYBER RISK

Companies must understand that cyber risk cannot be totally eliminated. Samit Soni, a Partner at Oliver Wyman, says that

"No institution has the resources to completely eliminate cyber risk"

A key part of managing cyber risk involves deriving a risk management strategy to quantify cyber risk to realize the benefits for comparison and justification of the level of investment towards mitigating it. Only with a price tag on risk can organizations determine which products, business lines or commercial strategies are worth the cyber risk they entail.

However, most organizations struggle with cyber risk quantification. Marsh conducted a survey of 300 leading risk executives and found that although 82 percent of respondents claimed to have conducted assessments to determine their vulnerability to cyberattacks, less than 40 percent have actually modeled potential losses.[35]

Modeling cyber risk exposure is critical, although not without challenges in execution. These challenges include determining the modeling methodology, obtaining the data necessary for modeling and making sound decisions in view of the lack of transparency.

Challenge #1: Modeling framework and development

The first step for organizations in cyber risk quantification is determining how to construct their model in a manner that generates a meaningful outcome. Companies have typically quantified cyber risks the same way they model other operational risks – focusing only on direct revenue losses. This definition is too narrow and does not accurately capture the full spectrum of losses that occur in an actual cyberattack.

While estimating the true cost of a potential cyber breach will never be an exact science, Oliver Wyman found that a more robust methodology involves developing scenarios that consider the risks from various angles – foregone revenue, liability losses, reputational damage, impacts to customers and processes, as well as regulatory requirements. In the event of a cyberattack, companies are hit with lost revenues as well as additional remediation costs, such as regulatory fines, and compensation to customers whose data is compromised. Finally, companies should project the amount of future revenue declines as a result of reputation damage.

Challenge #2: Data availability and reliability

A key challenge to quantifying and modeling cyber risks is to gather and collect all relevant data, both internal and external records of business, as well as operational and technical, so as to model against a range of expected and worst-case scenarios. External data is generally difficult to obtain in APAC due to the lack of transparency surrounding cyberattacks. While global benchmarks are available and can be used as proxies, their relevance to the region is questionable.

Beyond the APAC-specific issue of inadequate current data, the recent nature of cyber threats means historical data is also scarce. Consequently, companies face the challenge of making the right assumptions in their models. The extensive application of assumptions and parameters on models built for the region is thus expected to continue for some time. Meanwhile, companies are best served by relying on the educated assumptions of third-party experts to support their model build.

Challenge #3: Decision-making – lack of transparency and incomplete information

Compounded by the challenges in obtaining complete data and drawing sound assumptions for a robust scenario analysis, organizations may find it difficult to accurately price their risk exposure and consequently struggle to make strategically sound, risk-adjusted decisions. This is further reason for governments to drive more promote transparency.

Undoubtedly, the information provided from a robust model is critical for management to obtain a full view of the cyber risk, assess the adequacy of their risk protection and determine the necessity for further investments – all key tenets of a cyber risk strategy. Although challenging, companies cannot afford to ignore quantifying cyber risk, given its importance in the risk management process.

RECOGNISING THE ROLE OF INSURANCE

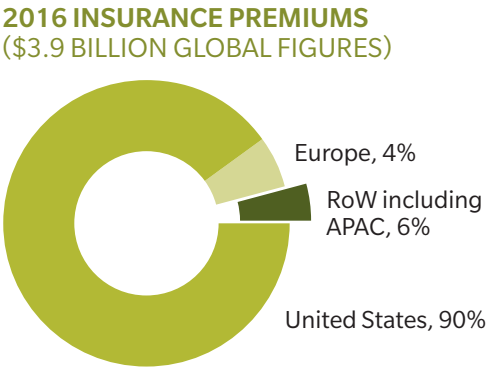
A key role of insurance is risk transfer. Having recognized that cyber risk cannot be eliminated; companies must be prepared for a cyberattack. The challenge with cyber risk is that it has the potential to be a tail risk to data, reputation, or the ability to do business. A 2016 study by Ponemon found that that the average total cost of a breach is $4 million, up 29 percent since 2013 and persistently rising.[43] The magnitude of a potential, sudden loss forces firms to scrutinize their ability to withstand such impact, and after rigorous analysis, part of the solution almost always involves looking to insurance as a way of transferring the risk away.

The role of cyber insurance is also useful in quantifying the price of cyber risk. Insurance premiums can serve as benchmarks to the risk modeling output and should be used as part of profitability analyses to determine the financial feasibility of a project, or executing cyber risk mitigation efforts. For instance, if a cybersecurity feature costs less than the net present value (NPV) of the resulting reduction in cyber insurance premiums, it is a worthwhile endeavor.

Prompted by the wave of high profile attacks and new data protection rules introduced around the world, annual gross written cyber insurance premiums have grown by 34 percent per annum over the last seven years, from $500 million in 2009 to $3.9 billion in 2016. Strong and long-term growth is expected in the global cyber insurance market, which is projected to reach $9 billion by 2020.[44]

However, the cyber insurance market remains heavily skewed towards the US: Insurance take-up rate was 55 percent in the US in 2016, compared to 36 and 30 percent in the UK and Germany respectively.[45] The take-up rate in APAC was even lower even though data is scarce. The distribution is worse for cyber insurance premiums, which was again largely dominated by the US (Exhibit 7).

Exhibit 7: Global cyber insurance market



The US is expected to continue dominating the global cyber insurance market over the next few years. A key driving force is the mandatory breach notification laws, the first of which was enacted in California in 2002. Today, 47 out of the 50 US states have enacted the legislation,[46] following the basic tenets of California's original law.

Despite the proliferation of technology and cyberattacks in APAC, there lies significant opportunities for insurers here since APAC's cyber insurance market share remains negligible.

This suggests strong growth potential and significant opportunities for insurers in the region–the cybersecurity market in APAC is projected to grow over 15 percent per annum till 2019. Munich Re expects Asian market volumes for cyber covers to grow to $1.5 billion by 2020, while AIG estimates cyber insurance penetration in Singapore could increase to 40 percent in 2020 from 9 percent today.

There are key insurability challenges that need to be addressed so insurers can fully capture the growing market share, while the insured are adequately protected at fair prices.

43 Ponemon Institute, 2016. Cost of Data Breach Study.
44 Munich Re, 2016. Innovation@Work.
45 Hiscox 2017. Cyber Readiness Report.
46 National Conference of State Legislatures, 2017. Security Breach Notification Laws.

Challenge #1: High specificity and strict limitations in cyber insurance product offerings

The scope of cyber insurance coverage remains highly specific as the characteristics of cyber threats across geographical locations, industries, and size of corporations vary widely (Exhibit 11). With little standardization across the products offered, companies need to have a deeper understanding of their own cyber risk exposures to determine the appropriate type and amount of coverage required based on their own risk tolerances. However, 49 percent of respondents surveyed by Marsh admitted that they possess "insufficient knowledge" about their own risk exposures to assess the insurances available.

Thus, even corporations with some form of cyber insurance may be unprotected against indirect losses that cannot be measured (reputational losses, for example), or not relevant to their risk exposure, leaving many corporations exposed to larger losses. On the other hand, cyber policy limits from a single underwriter typically range up to $100 million. Furthermore, with layered programs, a consortium of insurers and reinsurers can provide a tower of cyber insurance easily beyond $500 million in limits, which usually involve a series of insurers writing coverage each one in excess of lower limits written by other insurers.[47]

It is imperative that companies put in place processes for proper assessment of their cyber risk exposure, as that will lead to more targeted and effective mitigation, and greater ability to judge the value of the risk transfer options available in the market.

Douglas Ure, Practice Leader (Asia) at Marsh Risk Consulting, highlights that

"Cyber insurance is not a holistic solution in dealing with cyber exposure and covers only certain specific events and outcomes."

There is no one standard policy to cover cyber risk as the characteristics of cyber threats vary widely across industries and corporation size, while the terms and coverage of policies are complicated in nature. Thus, companies need to have a deeper understanding of their own exposure as it will help determine the appropriate type and amount of coverage required based on their risk tolerances (Figure 8 provides an example of different loss categories deriving from cyberattacks and non-malicious IT failures).

47 Marsh, 2015. UK Cyber Risk Survey.

Exhibit 8: Different loss categories available in the cyber insurance market

 **Intellectual property (IP) theft**	• Loss of value of an IP asset, expressed in terms of loss of revenue as a result of reduced market share
 **Business interruption**	• Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a results of cyberattacks or other non-malicious IT failures
 **Data and software loss**	• The cost to reconstitute data or software that has been deleted corrupted
 **Cyber extortion**	• The cost of expert handling for a extortion incident, combined with the amount of the ransom payment
 **Cyber crime/cyber fraud**	• The direct financial loss suffered by an organization arising form the use of computers to commit fraud or theft of money, securities or other property
 **Breach of privacy event**	• The cost to investigate and respond to a privacy breach event, including IT forensics and notify affected data subjects • Third-party liability claims arising for the same incidents. Fines from regulators and industry associations
 **Network failure liabilities**	• Third-party liabilities arising from certain security events occurring within the organization's IT network or passing through it in order to attack a third party
 **Impact of reputation**	• Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event
 **Physical asset damage**	• First-party loss due to the destruction of physical property resulting from cyberattacks
 **Death and bodily injury**	• Third-party liablity for death and bodily injuries resulting from cyberattacks
 **Incident investigation and response costs**	• Direct losses incurred in investigating and "closing" the incident and minimizing post-incident losses. Applies to all the other categories/events

Challenge #2: Evolving nature of technology and the Internet

The rapidly evolving nature of the Internet sets the speed not just for technological advancements but also severe cybercrimes with increasingly complex capabilities. Insurers need to constantly adapt to the dynamic digital landscape to improve their risk exposure models when designing more innovative cyber insurance products.

The constantly evolving nature of exposure also limits the usefulness of any historical data gathered, since they are most likely not going to be representative of future projections, hampering the development of accurate and robust models.

The low take-up rates of cyber insurance are often attributed to the mismatch of needs and offerings between the insured and the insurers. Whether it is in addressing the overpriced premium for a limited coverage, or offering products offered are better-suited and without many exclusion clauses, it is imperative for insurers to innovate and work on bridging the expectation gap.

One potential innovative product is a shared limits policy amongst firms with non-correlated risk. Marsh believes this should provide firms with access to $1 billion or more of coverage at a fraction of the cost of a stand-alone policy, sufficient to protect against a worst-case scenario. In 2016, Marsh launched Cyber ECHO, a global excess cyber risk facility underwritten by Lloyd's of London syndicates, offering up to $50 million in follow-form coverage for clients across all industries around the world.

Challenge #3: Expanding cyber insurability

Risk pooling has become an ineffective diversification mitigation tool in the cyber insurance landscape due to the underwhelming market share and smaller-than-required risk portfolios. Conventional strategies such as geographic or industrial diversifications also present greater challenges for cyber insurance as compared to other traditional insurance policies.

Tom Ridge, former Secretary of the US Department of Homeland Security, recently highlighted a key role for insurance-linked securities (ILS) in enabling cyber risks to be transferred to capital market investors. With growing cyber threats in terms of both systemic risks and financial impacts, the insurance industry alone may not be able to fully absorb the risk transfer.

Thus, it becomes critical for the insurance industry to innovate beyond the usual underwriting, and into the broader landscape involving capital markets, industries, and governments. This public-private partnership approach allows stacking multiple layers of both coverage and liquidity in the fight against cybercrimes.

Michael Owen, Chief Actuary from Guy Carpenter concurs:

"To meet the growing needs of our customers, Guy Carpenter is expanding our expertise in assessing cyber risk by working closely with external experts and industry players"

Without a doubt, insurance has a key role to play in cyber risk management. However, organizations need to be cognizant that a cyber insurance policy is one of the many tools that form a more comprehensive cybersecurity management strategy. Business executives need to find the right balance between cybersecurity investments and securing appropriate insurance plans suitable to the unique needs of their industry or organization.

CYBER RISK AND INSURANCE FOR SMEs

Cyber risk is both a growing risk for large companies and a rising concern for small- or medium-sized enterprises (SMEs). Cyber risk may indeed be more elevated for SMEs, as they can be less resilient than larger corporations due to greater reliance on data to provide services to customers, having less sophisticated systems and technology, lack of internal resources, using untrusted outsourced partners, and greater dependence on a smaller number of customers. These issues highlight the heightened risk and the need for overall resilience for SMEs to protect themselves and recover quickly if a cybersecurity breach occurs.

It is therefore unsurprising that concern amongst SMEs in APAC is rising. For example, a recent survey conducted by Beazley, in partnership with the Singapore Business federation (SBF), found that cybersecurity is one of the biggest concerns to Singapore-based SMEs.[28] The reality across APAC is similar to the perceived risk in Singapore, with increasingly more companies exposed to cyber breaches.

With the accelerated pace of technological change and investments being made to further innovate, all organizations need to ensure their risk management strategies are aligned with such change. This can, however, be overwhelming for SMEs, with the investment needed to protect against increasingly sophisticated attacks much greater

Insurance is being seen as a more valuable risk management tool for SMEs, with some Asia-based insurers developing tailored products for the SME segment. Investing in risk management and effective internal controls are also critical, but they will not eliminate the risk completely and the question of "not if, but when" will often re-emerge. Marsh cyber specialists have been working with SMEs to understand risk profiles and provide advice on preventative risk management strategies to determine the efficiency and cost effectiveness of the bespoke insurance plans.

Cyber insurance adoption in Singapore's SMEs generally remains below 10 percent, with less than 5 percent of manufacturing companies holding such policies compared to 35 percent or more companies in the financial services, technology, and telecommunications sectors. Similar to Singapore, only 14 percent of Australian small businesses held cyber insurance policies in 2016, although 19 percent surveyed are looking to purchase cyber insurance in the coming year.[48]

Cyber insurance premiums and coverage will vary, dependent on industry, risk profile and risk controls. For example, an SME in the manufacturing sector may identify cyber scenarios and quantify the risk with a potential $1 million impact. This may result in a premium of $15,000 for an insured limit of $1 million, providing peace of mind to the insured and providing a sensible cost-effective risk transfer solution. However, the situation may be completely different for a similar sized company in the technology sector, where the business model is built on data and the potential risk exposure is far greater. The premium spend may not be within the risk appetite of the company and the risk is fully retained. Without appropriate cyber risk controls in place, the tech-company is potentially exposed to a killer risk – resulting in a catastrophic failure of the business.

Cybercrimes can pose higher threat levels to SMEs in the way that it is less likely to do so for larger organizations with greater buffers and wider resources.

48 Security Brief AU, 2016. Cyber insurance in Australia set to rise in the wake of increasing attacks.

RECRUITING AND RETAINING CYBERSECURITY TALENT

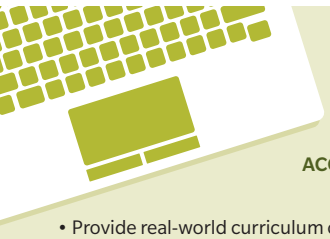
Another cog in the development of cyber-resilience is finding and keeping cybersecurity talent. A company can have the best cybersecurity policies, governance structures and processes in place, but without the people with requisite skills to execute the job, gaping holes will continue to exist in their cyber defense.

Burning Glass Technologies found that cybersecurity job postings have grown 74 percent between 2007 and 2013.[49] Low supply compounded by growing demand has led to intensifying competition for cyber talent, with 86 percent of companies indicating their intent to increase spending on cybersecurity staffing over the next 12 months.[13]

As companies look to increase cyber-resilience, it is important that the resources are invested beyond technology, governance and processes, and into the human capital that drives them as well.

Mercer recommends companies adopt the following three elements to gain the upper hand in the competition for recruiting and retaining cybersecurity talent:[50]

RECOMMENDATIONS FOR FUTURE DEVELOPMENTS IN ASEAN



PARTNERING WITH TERTIARY INSTITUTIONS AND BROADEN ACCESS TO NEW HIRES

- Provide real-world curriculum challenges, on-site job rotations, networking opportunities, co-ops, and internship opportunities that will provide young workers the development experience they need and the exposure hiring organizations require
- Establish a strong presence at universities and it will pay dividends beyond the immediate hires – students are likely to continue looking upon companies favorably even after many years from graduation

ENTICING CAREER PATH TRAJECTORIES AND ATTRACTIVE COMPENSATION PACKAGES

- Low compensation package and the absence of fast career paths were found to be top two most cited reasons for cyber talent attrition.[52]
- Create a visible, enticing and attainable internal career map to address the concern. This can be supplemented by creating opportunities to highlight accomplishments and to provide accelerated growth paths that align with employees' career goals

PROVIDING CONTINUOUS TRAINING AND BUILDING LINE OF BUSINESS EXPERIENCE

- Provide training opportunities to IT staff on business strategy, negotiation, legal considerations, communications, along with stronger ties to senior management
- Enable cybersecurity leaders to translate corporate business strategy into risk and cybersecurity resource plans for greater empowerment and ownership

49 Burning Glass Technologies, 2014. Job Market Intelligence: Report on the Growth of Cybersecurity Jobs.

50 BRINK News, 2016. Fighting for Cyber Talent in a Competitive Market.

EVALUATING THE EFFECTIVENESS OF YOUR CYBER DEFENSE

After applying an enterprise-wide cyber risk management framework and hiring the right people to build strong cyber defense, one further challenge for organizations is to understand how their holistic defense holds up against cyber adversaries.

Organizations that prepare for a cyberattack should undergo an assessment to understand their cybersecurity competency. Enter the white hats, professional hackers who use their abilities for ethical and legal purposes, and are available to test organizations' computer security systems and improve their defenses.

One such organization in the region is FireEye, which provides products and services to protect against more complex cyber threats, such as advanced persistent threats and spear phishing. Collaboration between FireEye and Marsh, for example, led to the creation and provision of an innovative service in 2015, the Cyber OASIS (Objective Assessment Scorecard of Information Security),[51] which is designed to provide organizations an objective assessment of their cybersecurity readiness to identify weaknesses that can be addressed.

51 Business Wire, 2015. Marsh and FireEye Collaborate to Offer Cybersecurity Readiness Service.

CONCLUSION: THE ROAD AHEAD

The APAC region has never been more vulnerable to cyberattacks; high value targets in a low security environment have turned the heads of cybercriminals. Change is required, and the responsibility falls upon the shoulders of governments, companies, and individuals alike.

Particularly in APAC, the potential of cyber threat exposure is disproportionally large compared to the amount of investments in cybersecurity or risk management strategies by governments and corporations. This imbalance may mostly be attributed to the lack of transparency, which significantly alters the perceptions of key decision makers, and undermines the severity of ever-present and ever-growing cyber threats.

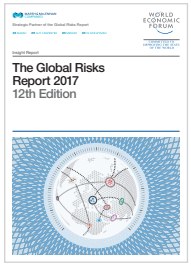
Yet, the region should take comfort in the fact that there are plans for considerations to improve cybersecurity by some more forward-looking governments. Recent examples include Australia's Data61 cybersecurity mega-hub established in 2016; Singapore-based Asia-Pacific Regional Intelligence and Analysis Centre as a private-public information sharing platform, to be in operation by mid-2017; and India building their in-house cyber talent pool by 2018, to name a few.

In addition, cyber insurance is both a useful mechanism for risk transfer and risk quantification tool to determine the amount of investments needed for a more comprehensive cybersecurity strategy. The concept of an enterprise-wide cyber risk management framework is also becoming a hot topic of discussion in more progressive Asian economies. However, more ought to be done to address corporate board indifference through increasing the degree of transparency.

Clearly, a lot more work is required. Governments need to find ways to effectively implement and enforce breach disclosure laws; companies must renew longentrenched approaches to cybersecurity; while individuals have to play their part and practice good cybersecurity habits.

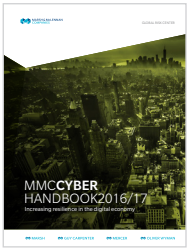
Stakeholders in APAC must recognize the urgency for change and embark on their own journey towards cyber resiliency to prevent further high-loss attacks. The road ahead is long and will be challenging, but investments today will be worthwhile.

RECENT PUBLICATIONS
FROM MARSH & McLENNAN COMPANIES



GLOBAL RISKS REPORT 2017

The 12th edition of the Global Risks Report identifies top concerns and risks trends over the next decade, including exploring the relationship between global risks and the emerging technologies of the Fourth Industrial Revolution.



MMC CYBER HANDBOOK 2016/17

The handbook includes articles, report extracts, and perspectives from cyber leaders and leading experts, providing new insights to strengthen cyber risk management approach to succeed in the emerging digital environment

EVOLVING RISK CONCERNS IN ASIA-PACIFIC

With Asia-Pacific emerging as the powerhouse of global growth, starting 2016 Marsh & McLennan Companies' Asia Pacific Risk Center will be publishing the "Emerging Risk Concerns in Asia-Pacific", drawing upon insights from the Global Risk Report and providing views on cyber-attacks, one of the highest-priority risks for the region.

EVOLVING CHALLENGES IN CYBER RISK MANAGEMENT – PROTECTING ASSETS AND OPTIMIZING EXPENDITURES 2016

Overview of shifting cyber threats and how companies should prepare them

THE ROAD TO RESILIENCE: MANAGING CYBER RISKS 2016

This report investigates how cyber risks can best be managed, taking into account the changing nature of the energy industry and energy infrastructure.

CYBER THREATS: A PERFECT STORM ABOUT TO HIT EUROPE?

The intensifying cyber threat environment and the evolving regulations challenge the cyber-preparedness of businesses across Europe; this report illustrates how companies must work to confront and avoid this imminent cyber storm cloud.

CYBER RESILIENCY IN THE FOURTH INDUSTRIAL REVOLUTION 2016

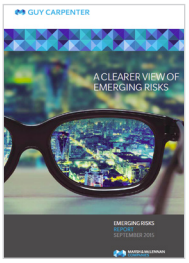
Provides a roadmap for global leaders facing emerging cyber threats in the hyper-connectivity in the Internet-of-Things, and the Internet-of-Services.

CYBERCRIME IN ASIA: A CHANGING REGULATORY ENVIRONMENT

Enterprise losses from cybercrime in Asia are the highest in the world, accounting for $138 billion in 2014. This report summarises recent cybercrimes in Asia and the corresponding responses by governments.

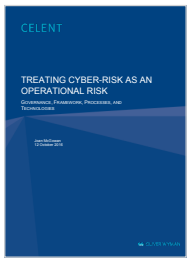
CLOSING THE DOOR TO CYBER ATTACKS: HOW ENTERPRISES CAN IMPLEMENT COMPREHENSIVE INFORMATION SECURITY

This report studies how organisations' attitudes towards the threat cyber risks pose, processes in place to manage them, and overall understanding and use of cyber insurance as a means of risk transfer.



AHEAD OF THE CURVE: UNDERSTANDING EMERGING RISKS

This report provides a deep-dive analysis on cyber risks, which pose a set of aggregations of risk that spread beyond the corporation to affiliates, outsources, counterparties, and supply chain.



TREATING CYBER-RISK AS AN OPERATIONAL RISK

This report examines the touch points and convergence of cybersecurity and operational risk functions and controls.

HUMAN CAPITAL CHALLENGES IN A HIGH-RISK ENVIRONMENT: 2015 CYBER SECURITY TALENT SPOT POLL

To help clients grapple with maintaining cyber security, Mercer conducted a Spot Poll to understand organisational responsibility for cyber security, resources allocated to cyber security, and the challenges of recruiting and retaining cyber security talent.

To read the digital version of the Cyber Risk in Asia Pacific publication, please visit **www.mmc.com/asia-pacific-risk-center.html**

Authors

WOLFRAM HEDRICH
Executive Director, APRC
wolfram.hedrich@mmc.com

GERALD WONG
Senior Consultant, Oliver Wyman
gerald.wong@oliverwyman.com

JACLYN YEO
Senior Research Analyst, APRC
jaclyn.yeo@mmc.com

Marsh & McLennan Companies Contributors

Marsh & McLennan Companies: Alex Wittenberg, Richard Smith-Bingham, Lucy Nottingham, John Craig; **Marsh:** Douglas Ure, Richard Green, Arati Varma; **Mercer:** Vidisha Mehta, Godelieve van Dooren, Kate Bravery; **Oliver Wyman:** Claus Herbolzheimer, Samit Soni, Wei Ying Cheah; **Guy Carpenter:** Michael Owen, Vivian Wesson, Teresa Aquilina.

The design work for this report was led by Chen Min Chan and Doreen Tan, Oliver Wyman.

About Marsh & McLennan Companies

MARSH & McLENNAN COMPANIES (NYSE: MMC) is a global professional services firm offering clients advice and solutions in the areas of risk, strategy and people. Marsh is a leader in insurance broking and risk management; Guy Carpenter is a leader in providing risk and reinsurance intermediary services; Mercer is a leader in talent, health, retirement and investment consulting; and Oliver Wyman is a leader in management consulting. With annual revenue of $13 billion and approximately 60,000 colleagues worldwide, Marsh & McLennan Companies provides analysis, advice and transactional capabilities to clients in more than 130 countries. The Company is committed to being a responsible corporate citizen and making a positive impact in the communities in which it operates. Visit www.mmc.com for more information and follow us on LinkedIn and Twitter @MMC_Global.

About Asia Pacific Risk Center

Marsh & McLennan Companies' Asia Pacific Risk Center draws on the expertise of Marsh, Mercer, Guy Carpenter, and Oliver Wyman, along with top-tier research partners, to address the major threats facing industries, governments, and societies in the Asia Pacific region. We highlight critical risk issues, bring together leaders from different sectors to stimulate new thinking, and deliver actionable insights that help businesses and governments respond more nimbly to the challenges and opportunities of our time. Our regionally focused digital news hub, BRINK Asia, provides top executives and policy leaders up-to-the-minute insights, analysis, and informed perspectives on developing risk issues relevant to the Asian market.

For more information, please email the team at contactaprc@mmc.com.

Economy • Environment • Geopolitics •
Society • Technology

BRINK Asia is a digital news platform that provides regional perspectives from leading experts on issues related to emerging risks, growth and innovation.

contact@brinkasia.com
www.brinknews.com/asia
Follow BRINK Asia on Twitter
Follow BRINK Asia on Linkedin

This is made possible by Marsh & McLennan Companies and managed by Atlantic Media Strategies

www.mmc.com

MARSH