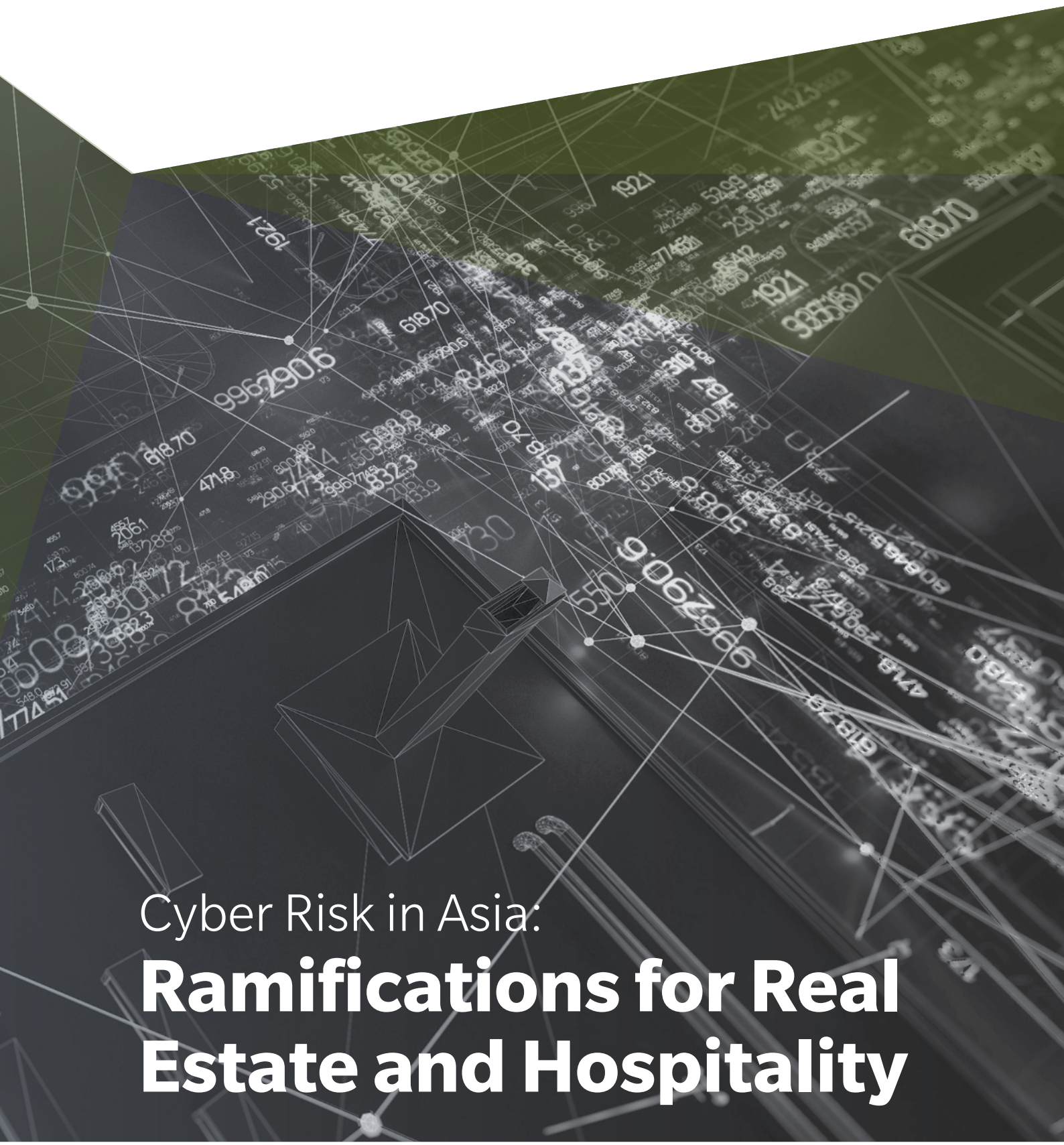
MARSH & McLENNAN COMPANIES | Asia Pacific Risk Center



Cyber Risk in Asia: **Ramifications for Real Estate and Hospitality**

MARSH OLIVER WYMAN MERCER GUY CARPENTER

TABLE OF CONTENTS

Key Takeaways 1

1 The Cyber Threat Landscape 2

2 Asia Remains ill-prepared for Cyber Risk Events 3

3 Real Estate and Hospitality – At the Crossroads of Emerging Technologies and Cyber Risks 4

Attractive Key Targets 5

Vulnerable Entry Points 6

4 Case Examples of Cyber Incidents 8

5 Asia's Real Estate and Hospitality Sector is Under-prepared 11

The Widening Perception-reality Gap 11

Insufficient Defense Against the Expanding Attack Surface 12

Indifference Towards Purchasing Cyber Insurance 13

6 Getting Cyber-ready 15

Embed Cyber in Enterprise Risk Management Plans 18

Strengthen Cyber-secure Culture 18

Transfer Residual Risks That Cannot be Eliminated 18

7 Concluding Remarks 19

8 Methodology 20

KEY TAKEAWAYS

1. Cyber risk continues to rank among the top business risk concerns globally in 2017, as most businesses around the world look to prepare themselves for the next large cyber-attack.

2. Organizations across Asia are vulnerable to cyber-attacks as the region remains ill-prepared for cyber incidents. This is primarily due to the absence of a rigorous regulatory environment, a low level of investment in cybersecurity, and the inherent shortage of talent.

3. In this age of rapid digital transformation, major industry sectors, such as real estate and hospitality (RE&H), increasingly find themselves at the cross roads of increased usage of emerging technology and growing cyber risks—making them attractive targets for cyber criminals.

4. Unfortunately, the RE&H sector lacks the necessary cyber preparedness and most organizations are not as cyber risk-ready as they should be. This was made clear by the results of both the *Marsh/Microsoft Global Cyber Risk Perception Survey 2017 and the Marsh Hong Kong Cyber Risk Survey 2017*.

5. While many respondents whose businesses are in the RE&H sector in Asia are confident their organizations understand the cyber risk exposure, our surveys reveal a widening perception-reality gap and insufficient defense strategies against the expanding attack surface. These findings suggest a wide chasm between how prepared businesses think they are for an attack and how protected they truly are.

6. The RE&H sector in Asia also appears to be indifferent towards purchasing cyber insurance, with more than a third of the respondents indicating that their organization either do not have cyber insurance, have no plans to purchase any, or that they do not know whether their organizations have cyber insurance.

7. Businesses ought to become more cyber-ready as key trends suggest that the RE&H sector is increasingly exposed to cyber vulnerabilities. They can strengthen their cybersecurity posture by embedding cyber in enterprise risk management plans, building a cyber-secure culture within the organization, and leveraging risk transfer through cyber insurance policies.

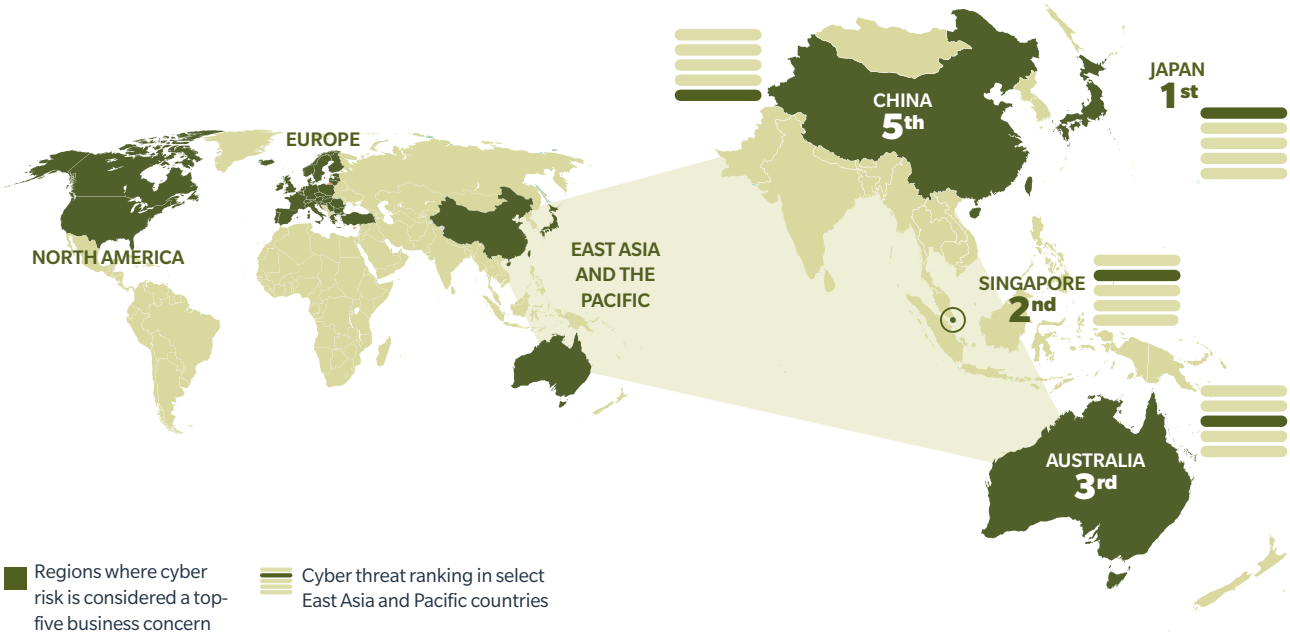
THE **CYBER THREAT** LANDSCAPE

Unsurprisingly, cybersecurity breaches are a top business risk concern globally. With a spate of cyber-attacks spreading around the world, cyber risk has climbed higher atop the ladder of C-Suite executives' priorities in 2017.[1] Cyber risk ranks 8th on the 2017 World Economic Forum's list of risks in doing business—up three places from 2016.[2] Exhibit 1 highlights the regions where cyber is ranked among the top five risks, with the country level breakdown by rank order in East Asia and the Pacific.

Owing to incidents such as the WannaCry hack and the Equifax breach,[3] most businesses around the world are looking to prepare themselves for the next large cyber-attack, as well as for the reputational and legislative fallout that often follows.

EXHIBIT 1: CYBER RISK PRIORITIZATION AMONG GLOBAL BUSINESS LEADERS
Sources: APRC

Large cyber-attacks ranked **8th** on a list of top global risks or concern to business



[1] World Economic Forum, 2017. The Global Risks Report 2017.

[2] BRINK News, 2017. Politics and cyber are rising concerns for business leaders.

[3] Oliver Wyman, 2017. The Equifax data breach: and its impact on identity verification.

ASIA REMAINS **ILL-PREPARED** FOR CYBER RISK EVENTS

Firms across Asia are particularly vulnerable to cyber-attacks, largely due to their lack of preparedness. Statistics show that hackers are 80 percent more likely to attack organizations in Asia [4]—primarily due to the absence of a rigorous cyber regulatory environment and low investment levels in cybersecurity across the region.[5] The shortage of cybersecurity talent is also significant, especially in Asia—42 percent of human resources professionals anticipated an under-supply of cybersecurity professionals in 2017, for example, with the numbers for Japan and China standing out at 48 and 56 percent respectively.[5]

Asian firms spend relatively less on information technology security and take almost twice as long to respond to a data breach as compared to their global peers, facing frequent and damaging cyber-attacks (Exhibit 2). For example, 59 percent of Asian businesses experienced a cyber-incident on at least a monthly basis. [6] The threat Asian businesses face from cyber attackers is clearly potent, and yet, it is not being met with the necessary precautions.

Moreover, data breach notification laws are severely lacking across the region, resulting in cyber-attacks being under-reported or kept entirely under wraps. This undermines the ability of industry members to learn from one another and to prevent future attacks.

EXHIBIT 2: CYBER-ATTACKS AND SECURITY LEVELS IN ASIA
Sources: APRC analysis

Asian firms are **highly susceptible** to cyber-attacks...

Hackers are **80%** more likely to attack organizations in Asia

59% of Asian businesses experienced a cyber incident on at least a monthly basis in 2016

...and **yet**...

Asian firms spend, on average, **47% less on IT security** than North American firms

Asian firms take **1.7X** longer to respond to a breach compared to the global average

As technological advancement accelerates across the region, Asian businesses would do well to recognize that their vulnerability to cyber-attacks is set to intensify.

Several high-profile and unconcealable cyber-attacks appear to be changing this. The $81 million cyber-heist on Bangladesh's central bank in May 2016 and the global ransomware WannaCry attacks exactly a year after shocked the region, and gave the corporate world a timely reminder of the importance of addressing cyber risks.

As technological advancement accelerates across the region, Asian businesses would do well to recognize that their vulnerability to cyber-attacks is set to intensify.

[4] Marsh & McLennan Companies, 2017. Cyber Risks in Asia Pacific – the case for greater transparency

[5] Marsh & McLennan Companies, 2017. Evolving Risk Concerns in Asia-Pacific 2017.

[6] Telstra, 2017. Telstra Cyber Security Report 2017 – managing risk in a digital world.

REAL ESTATE AND HOSPITALITY – **AT THE CROSSROADS OF EMERGING TECHNOLOGIES AND CYBER RISKS**

As technology develops and pervades the RE&H sector, these vulnerabilities will also become more pronounced.

The emerging technologies of the Fourth Industrial Revolution (4IR) have transformed the world—the amount of data and information created, the speed and reach of Internet connectivity, and the immense computational power today, among others, are greater than ever before.

Artificial intelligence, the Internet of things (IoT), and cloud systems are just some of the innovative vehicles for productivity optimization across major industries such as financial services, healthcare, real estate and hospitality, among others (Exhibit 3). However, before deploying these emerging technologies to enable economic benefits, companies need to be cognizant of how digital transformation may present new challenges, as their internal processes and interactions with customers will now be considerably augmented.

EXHIBIT 3: ILLUSTRATIVE IMPACT OF EMERGING TECHNOLOGIES ON SELECTED INDUSTRIES
Sources: APRC, Oliver Wyman analyses

	Internet of Things (IoT)	Artificial Intelligence	Blockchain	Cloud Systems	Internet Access (WiFi Networks)
Energy	●	●	●	●	●
Transportation	●	●	●	●	●
Manufacturing & Construction	●	●	●	●	●
Financial Services	●	●	●	●	●
Healthcare	●	●	●	●	●
Real Estate	●	●	●	●	●
Hospitality	●	●	●	●	●

Estimated impact scale →

ATTRACTIVE KEY TARGETS

The real estate and hospitality (RE&H) sector[7] is susceptible to cyber-attacks (Box 1) due to the nature of its business. Businesses in this sector sit on vast treasure troves of financial assets, personal identifiable information (PII), external credit scores, and internal Intellectual Property (IP) data—making them a convenient target for perpetrators.

Box 1: Typical data types collected by the real estate and hospitality sectors

- **Personally Identifiable Information (PII)**: Data that would allow an attacker to impersonate another individual including using their identification numbers, names, addresses, passwords, financial details, family or personal details
- **Intellectual Property (IP)**: Confidential internal company information such as operating processes, negotiation strategies, building blueprints, and five-year-plans
- **Payment Card Industry information (PCI)**: Card numbers and pin information belonging to individuals
- **Privileged Information**: Confidential data belonging to external clients or vendors

Globally, the hospitality and retail sector is the fourth most frequently targeted industry, accounting for almost 11 percent of data breaches in 2016-2017.[8] As technology develops and pervades the RE&H sector, these vulnerabilities will also become more pronounced.

[7] In this paper, the real estate sector refers to the buying and selling of residential, commercial, and industrial properties, while the hospitality sector is broadly related to the service industry that includes segments such as accommodation, recreation, travel and tourism, and food and beverages.

[8] Verizon, 2017. 2017 Data Breach Investigations Report 10th Edition.

[9] Marsh, 2017. Marsh/Microsoft Global Cyber Risk Perception Survey.

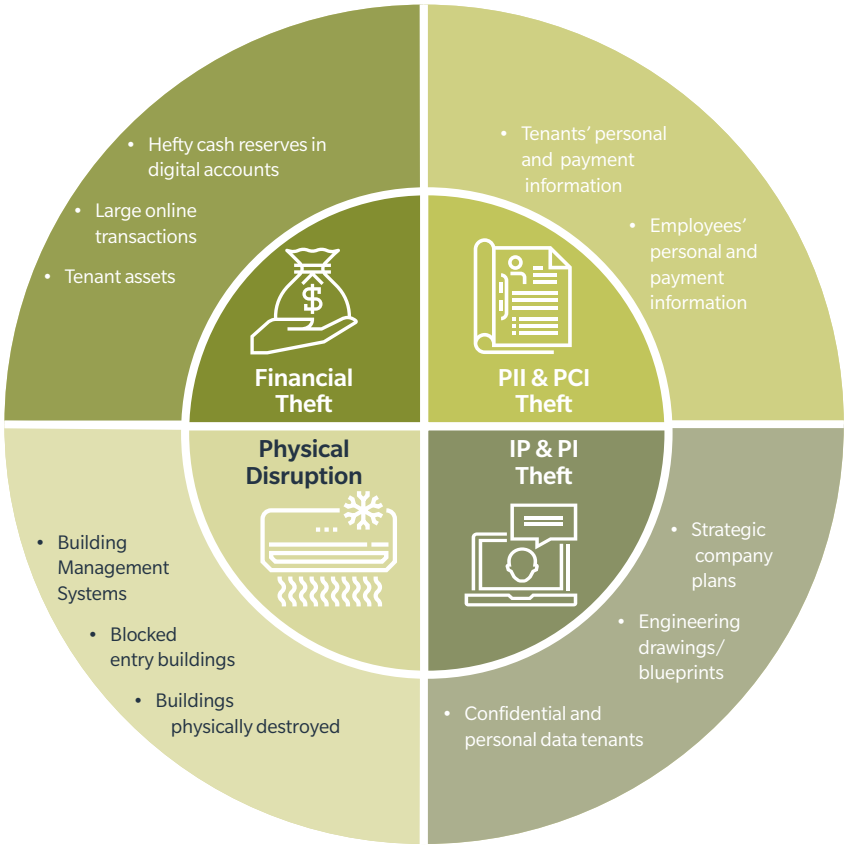
[10] Marsh, 2017. Marsh Hong Kong Survey: Managing Cyber Risk – Is your Organization Risk Ready?

In fact, findings from the Marsh/Microsoft Global Cyber Risk Perception Survey[9] and the Marsh Hong Kong Cyber Survey for the RE&H sector,[10] both administered between July and September 2017, have revealed that the level of cybersecurity preparedness across this sector in Asia is low.

Several studies have also shown that the primary target of cyber criminals in the hospitality sector is the financial assets of the everyday client assessed through credit card details, payer credentials, and other forms of PII. According to Verizon's 2017 data breach study, almost all the attacks launched on the hospitality sector were financially motivated and executed by criminal groups, which have become more sophisticated and organized. Approximately 87 percent of breaches are targeted at Points of Sale (POS) devices; hence it is unsurprising that identity data theft has consistently been the most common breach type since 2013. [11]

Real estate firms comprising construction and asset management, often consider themselves to be safe from cyber-attacks since they do not hold as much PII and PCI data as the other more consumer-facing industries. However, real estate firms also fall prey to several other sources of vulnerability (Exhibit 4). Moreover, as real estate firms adopt emerging technologies, PII and PCI data will increasingly come under the purview of real estate firms.

EXHIBIT4: PRIME DATA TARGETS FOR CYBER-ATTACKERS FOR THE RE&H SECTOR
Sources: APRC analysis



VULNERABLE ENTRY POINTS

With the onset of the 4IR, confidential information of both companies and end users is also becoming more exposed to criminal activity as the RE&H sector is becoming more connected to the Internet than ever. It is crucial for firms to note how their technology adoption is broadening their surface of attack, and for risk managers to identify vulnerable access points that can be exploited by cyber criminals.

Complications in terms of additional security may also be created without the companies knowing. For example, economic development and urbanization across Asia spurred by various smart city initiatives (Box 2) rapidly create additional data and connect that data to the built environment. Likewise, RE&H firms in the region will be increasingly developing, selling, and using buildings that are amassing vast amounts of sensitive and personal Big Data. These buildings centralize the collection of data across clients, vendors, and businesses, making them prime targets for attack.

As a result, increase in connectivity between the RE&H sectors and the built environment adds to the burden on firms to strengthen their cybersecurity measures and ensure adequate client-data protection.

[11] Gemalto, 2017. 2017 Poor Internet Security Practices Take a Toll.

Box 2: Cyber vulnerabilities and smart city initiatives

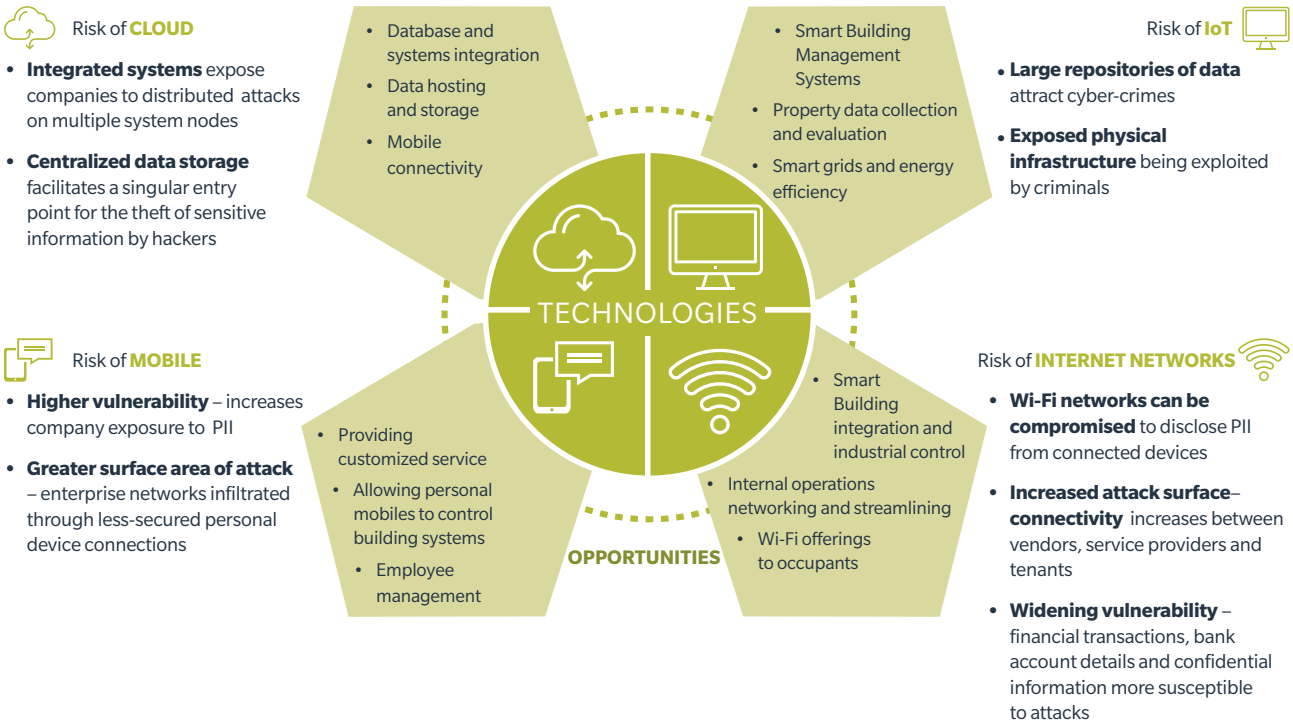
Globally, the push for smart cities is being fuelled in large part by the Asia-Pacific region. Between 2017 and 2021, for example, the Asia-Pacific market for smart city information and communications technology (ICT) infrastructure is expected to grow at a CAGR of 20 percent against the global average of 17 percent CAGR.[12]

The ability of individuals in the region to connect to smart buildings and transmit their data is also increasing dramatically. By 2020, Cisco expects 11.7 billion mobile devices in the Asia-Pacific region, up from 7.5 billion in 2015. As a result, internet traffic growth in the region will more than triple from 2015 to 2020, at 25 percent CAGR.[13] The PII that will resultantly be transmitted across these expanding networks will deepen immensely. In addition, populous nations such as China and India are undertaking country-wide digitized data collection programs —the biometric identification program in India,[14] and China's WeChat platform,[15] among others—making them more attractive targets to cyber criminals.

As countries in the Asia-Pacific region begin to focus on developing smart cities, data proliferation will expand exponentially, increasing the likelihood of Big Data getting more interlinked with RE&H systems and databases.

Exhibit 5 illustrates the four technologies currently being widely adopted across the RE&H sectors that can make companies more vulnerable. These technologies enable both the amassing and transmitting of Big Data and financial information, both of which pose prime targets for cyber-attacks. For instance, as more consumers browse and conduct transactions from their mobile devices, companies' and consumers' payment information will become more tightly interconnected, offering cyber-criminals a window of opportunity as a plethora of data and information is gathered. Eventually, this will lead to an exponential increase in the number of endpoints for potential attacks.

EXHIBIT5: RISKS AND OPPORTUNITIES IN ADOPTING EMERGING TECHNOLOGIES IN THE RE&H SECTOR
Sources: APRC analysis



[12] Technavio, 2017. Global Smart City ICT Infrastructure Market 2017-2021.

[13] 13 Cisco, 2016. Asia Pacific – 2020 Forecast Highlights.

[14] Unique Identification Authority of India, 2017. Aadhaar Trend.

[15] TChina Channel, 2017. 2017 WeChat User Behavior Report.

CASE EXAMPLES OF **CYBER INCIDENTS**

Despite the increasingly innovative techniques used in cyber-attacks, many attackers are still making use of traditional tactics to gain access. They are also targeting executives and other frontline employees to trick them into activating malicious software codes that provide easy access into an organization's network system. The following examples illustrate some old-school techniques used by cyber-attackers. However, the success or failure of these attempts is usually dependent on the level of preparedness and defense strategies of these targeted organizations.

EXAMPLE 1 ATTACK ON THE HKEX NEWS WEBSITE

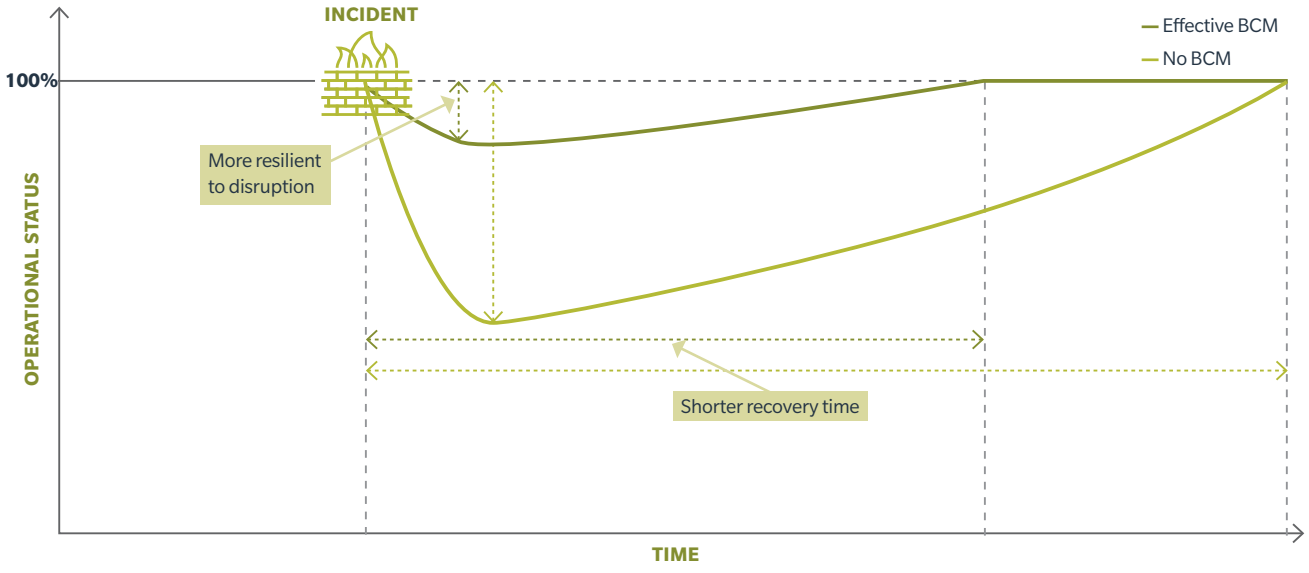
A sustained distributed denial of service (DDoS) attack from various sources with malicious intent was launched at the news website of the Hong Kong Stock Exchange (HKEx) over two days in August 2011,[16] which crashed the exchange's webpage that provided financial announcements and news updates. The incident prompted the HKEx to suspend trading of the affected companies. The HKEx news website returned to normal operations the next day despite a subsequent attack that consisted of a mixture of different attacking techniques.

The swift resumption of normal trading operations was attributed to the effective business continuity management plans. The exchange had identified and determined the criticality of every business function, such that the "mission-critical" systems used for trading, clearing, and distributing market data ran on a separate system not connected to the Internet, thus remaining largely unaffected by the DDoS attacks.

Usually, it can take up to two weeks or longer for full recovery of primary ICT systems. However, critical services such as the trading platforms and clearing systems can resume business activities within 24 hours, as soon as the business continuity plans are activated (Exhibit 6). Moreover, in such situations, backend functions and services that are not deemed to be critical during the cyber-attacks may be temporarily suspended while post-incident forensic investigations are ongoing. In the case of the HKEx incident, for example, the suspended news webpages were substituted by an older bulletin board for traders to obtain announcements being released by listed companies, so as to minimize any further trading disruptions.

[16] Financial Times, 2011. Hong Kong Exchange hit by hackers.

EXHIBIT6: MINIMIZED TRADING DISRUPTION THROUGH EFFECTIVE BUSINESS CONTINUITY PLANS
Sources: APRC analysis



EXAMPLE 2 ATTACK ON AN AUSTRALIAN REAL ESTATE AGENCY

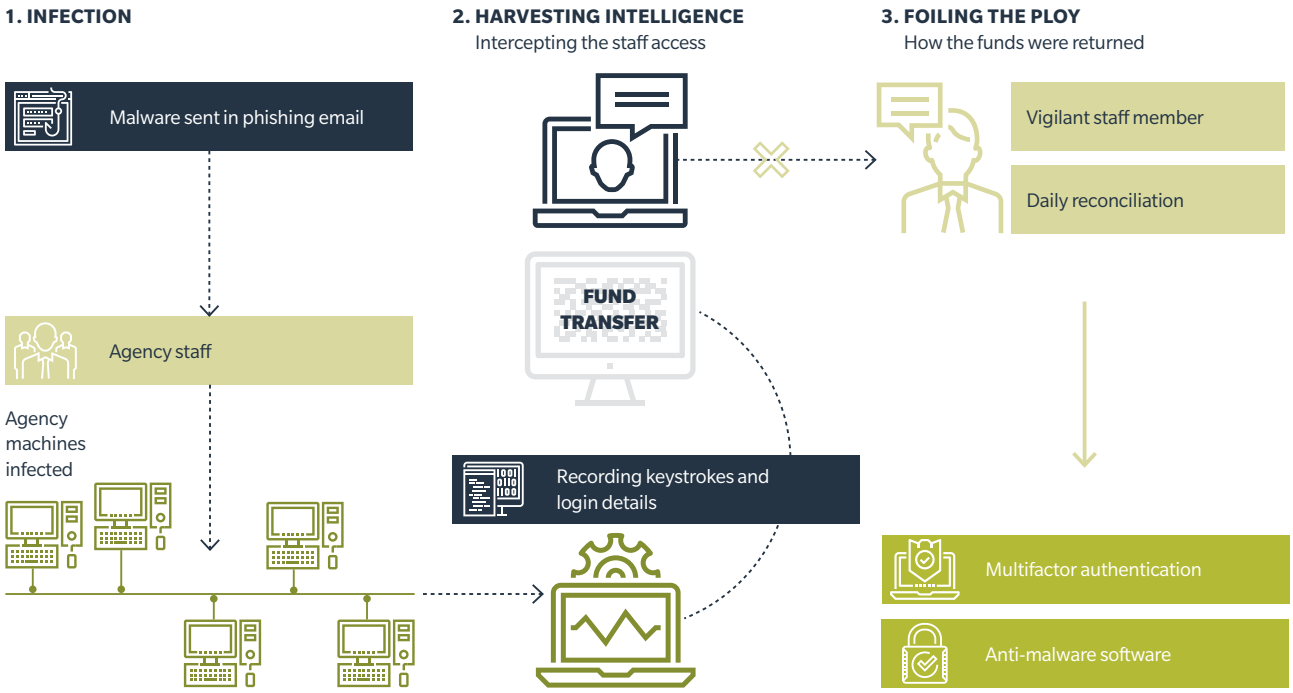
A Perth-based real estate agency faced near-theft in September 2016, when there was an unauthorized withdrawal request of A$500,000 (~US$384,000) from the agency's trust account. The cyber criminals had managed to install malware onto the firm's computer systems, which was believed to have infiltrated the system when staff members unknowingly clicked on malicious website links from phishing emails. Once installed, the malware allowed the criminals to record keystrokes and identify the firm's bank login details (Exhibit 7).

Fortunately, as part of the real estate agency's best practice to reconcile trust accounts daily, the unauthorized withdrawal was discovered in time by a staff member, and the relevant bank retracted the fund transfer before the funds reached the criminals.[17] Besides enhancing training programs to raise cybersecurity awareness and educating employees to recognize malicious phishing emails, the real estate firm subsequently introduced a more secure network connection to its bank, which included anti-malware software, and multi-party and multifactor authentication features.

This may be considered a lucky episode to some, but the worrying trend is that real estate agencies are becoming the latest targets of cyber thieves. Among the many attempted cyber intrusions in 2015 and 2016, two other real estate agencies that were less fortunate lost a total of A$100,000 due to fraudulent online transactions.

[17] Government of Western Australia, 2016. Attempted theft of $500,000 in cyber-attack on real estate agency.

EXHIBIT7: HOW THE STOLEN FUNDS WERE RETURNED TO THE REAL ESTATE AGENCY
Sources: APRC analysis



EXAMPLE 3 THE DOUBLE-BILL HOTEL CHAIN HACK

A reputable hotel chain suffered two data breaches in 2015[18] and in 2017[19] when its cybersecurity systems were compromised, leaking PII and PCI of their customers worldwide. While they suffered a considerable hit in 2015 as well, the impact on China and Hong Kong in the 2017 breach was significantly greater, illustrating that cyber threats are on the rise in Asia and impacting the region more than earlier. Both cyber intrusions were caused by malware that infected the hotel chain's payment processing systems, exposing PCI, such as cardholder names, card numbers, expiry dates and internal verification codes—all of which were obtained from credit cards manually entered or swiped at the front desks.

The POS malware breach was caused by an insertion of malicious software code from a third party onto several hotel IT systems via the POS computer. For both incidents (Exhibit 8), the company did not disclose how many customers were potentially affected and it did not know exactly whose details may have been compromised.

[18] South China Morning Post, 2015. Three Hyatt hotels in Hong Kong hit by malware designed to steal credit card data.

[19] Reuters, 2017. Hyatt Hotels discovers card data breach at 41 properties .

EXHIBIT8: SUMMARY STATISTICS OF THE HOTEL CHAIN HACK
Sources: APRC analysis

ASIA'S REAL ESTATE AND HOSPITALITY SECTOR IS **UNDER-PREPARED**

RE&H companies appear to be well aware of the disruption brought about by emerging technologies, but a majority of them are still largely unprepared for cyber-attacks. According to the Marsh Hong Kong Cyber Survey, half of our RE&H clients in Hong Kong revealed they have not implemented or conducted any cyber loss mitigation techniques, such as establishing a crisis management team or retaining forensic specialists, among others, over the past 12 months. This suggests that about 50 percent of them are not as risk-ready as they should be.

According to the survey results, the lack of cyber preparedness by the RE&H sector may be attributed to the following:

- A widening perception-reality gap
- Insufficient defense against the expanding attack surface
- Indifference towards purchasing cyber insurance

THE WIDENING PERCEPTION-REALITY GAP

Both our Marsh/Microsoft Global Cyber Risk Perception Survey as well as the Marsh Hong Kong Cyber Risk Survey show that there is a wide chasm between how prepared firms think they are for an attack, and how protected they actually are. For example, a large majority (65 percent) of respondents from the RE&H sector in Asia ranked cyber threat as a top-five corporate risk concern; but 85 percent of the surveyed RE&H respondents in Hong Kong spend less than 10 percent of their annual budget on cybersecurity.

Furthermore, firms in the RE&H sector appear mostly confident (88 percent) that they understand their cyber risk exposure, but almost half (48 percent) are either unaware of or do not have any methods to measure their cyber risk exposure.

EXHIBIT 9: COMPARISON BETWEEN PERCEPTION AND ACTUAL ACTIONS TAKEN
Sources: APRC analysis; Marsh Cyber Surveys dataset

	PERCEPTION	REALITY
1	**Cyber is top enterprise-wide risk** A significant proportion (65%) of respondents in the RE&H sector in Asia ranked cyber as either the top or among the top five risks in the organization's risk register *(Q: Among my organization's risk management priorities, cyber risk is)*	**Low annual budget spent** *85% of the surveyed respondents* indicated they spend less than 10 percent of their annual budget on cybersecurity investments *(Q: What percentage of your annual budget is allocated to cybersecurity?)*
2	**Confidence level is high** Respondents (38% and 50% highly and fairly confident) feel that their sector understands its cyber risk exposure *(Q: Please indicate your confidence in your organization's ability to understand its cyber risk exposure)*	**Lack of risk quantification** Almost half (48%) revealed they are either unaware of or their organizations do not have any methods to measure their cyber risk exposure *Q: How does your organization measure or express its cyber risk exposure?)*
3	**Response plans are unnecessary** A majority of respondents (60%) do not have or no not plan to develop a cyber incident response plan, primarily because respondents have faith in their security measures *(Q: If your organization does not have and/or does not plan to develop a cyber incident response plan, why not?)*	**High rates of attack on the RE&H sector** Over 20% of respondents reported to have suffered an attack in the last 12 months alone. This number does not account for undetected attacks *(Q: Has your organization been a victim of a successful cyber-attack in the past 12 months?)*

Survey respondents also assumed that their internal cybersecurity frameworks were sufficient to prevent cyber-attacks from happening. Six out of 10 RE&H companies do not have and do not plan to develop a cyber-incident response plan, despite one in five having responded that they had experienced a cyber-attack in the past 12 months alone. This suggests that despite a high chance of being attacked, a majority of the firms have not prepared to respond to an attack at all.

The widening perception-reality gap as shown in Exhibit 9 may be the leading factor resulting in the RE&H sector failing to recognize that cyber threat is an enterprise-wide risk.

INSUFFICIENT DEFENSE AGAINST THE EXPANDING ATTACK SURFACE

The most vulnerable entry points for cyber criminals are summarized in Exhibit 10, along with the steps taken to protect themselves, and existing barriers to implementing a rigorous response plan for respondents whose businesses are in the RE&H sector in Asia.

Our surveys showed that respondents recognize the areas where emerging technologies are resulting in a broadening of the attack surface, and driving new weaknesses in their traditional business models. Respondents in the RE&H sector in Asia are also able to accurately identify the key entry points (such as cloud and mobile applications, POS devices) specifically for their sectors.

Most respondents have also put in place some form of cybersecurity measures to protect against cyber-attacks—conducting cybersecurity gap assessments is the most common such measure employed by the surveyed business,

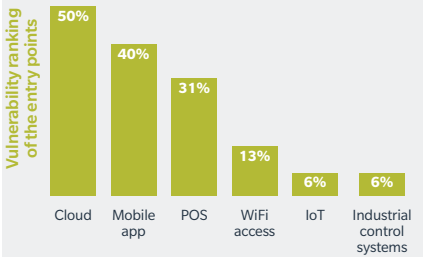
There is a wide chasm between how prepared firms think they are for an attack, and how protected they actually are.

followed by risk awareness training programs and encrypting mobile devices connected to the enterprise network. Nonetheless, almost half of the respondents either did not know of any steps their organizations had taken, or indicated their organizations had taken less than five of the potential steps to mitigate risks over the past 12 to 24 months.

EXHIBIT 10: CYBER DEFENSE STRATEGIES UTILIZED BY THE RE&H SECTOR
Sources: APRC analysis; dataset from Marsh Hong Kong and Marsh/Microsoft cyber surveys

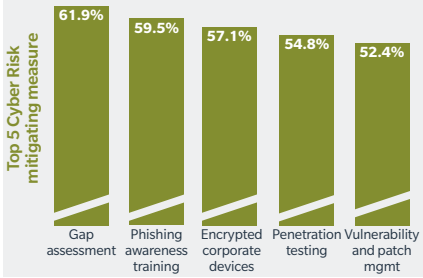
1 Identify Vulnerable Entry Points

Q: Which of the following entry points do you think are the most vulnerable in the RE&H sector?)
By percentage of respondents' selection



2 Mitigation Measures Taken

Q: Which of these steps has your organization taken in the past 12 to 24 months?
By percentage of respondents' selection



3 Cyber Incident Response Plan

Q: If your organization does not have and/or does not plan to develop a cyber incident response plan, why not?

Further, awareness of the widening attack surface is not matched with similar levels of defense. Sixty percent of organizations surveyed are without proper incident response plans; 10 percent cited the lack of expertise as one reason for not having an incident response plan, while another 10 percent suggested that cyber incidents are covered in other crisis plans and thus need not to be singled out as a standalone plan for incident response. Having cyber incidents covered in other crisis plans may result in far more complications—relying on a plan that focuses on other types of emergencies (such as fires, power outage)—since these plans do not critically address issues unique to information security breaches with internal stakeholders, or adequately communicate with affected clients the breached pathways and possible mitigating measures.

As a result, huge economic losses are highly likely to occur due to business interruption as critical functions, data protection, and loss prevention backup solutions may cease operations in the event of a cyber-attack. Without proper crisis management and stakeholder engagement, normal business operations will further be delayed as organizations scramble to carry out post-incident forensic investigations and notify affected individuals.

Besides the lack of incident response plans against cyber-attacks, 31 percent of those surveyed in the RE&H sector in Asia also do not assess external cyber threats coming from vendors, contractors, or suppliers, or do not know whether their organizations assess these external cyber threats. Without proper measures to mitigate against third-party risks, companies are leaving wide open the possibility of watering hole attacks.[20]

INDIFFERENCE TOWARDS PURCHASING CYBER INSURANCE

According to the Marsh surveys, cyber insurance adoption rates (33 percent) in the RE&H sector in Asia are on par with other mature markets such as the UK (36 percent) and Germany (30 percent), but lower than in the US (55 percent).[21]

As shown in Exhibit 11, just under a third of the respondents (31 percent) indicated that they have plans to purchase or increase cyber insurance over the next 12 months, primarily driven by internal cyber risk management plans, or prompted by successful cyber-attacks on other companies. In contrast, one in 10 RE&H companies do not have and do not intend to purchase cyber insurance coverage, citing limitations in coverage, cost considerations or the belief that cyber risk was adequately covered in other policies as key reasons.

It is unsurprising that regulatory factors such as legislations or rating agency standards have negligible impact on the decision to purchase insurance in Asia-Pacific, since legislation and enforcement are currently struggling to keep pace in this region. With the EU's General Data Protection Regulation (GDPR) coming into force in May 2018, cybersecurity laws and mandatory data breach disclosures across the region will look to rise. Further, regardless of location, any organization holding on to the personal data of any EU citizen will be affected by the GDPR. As such, cyber insurance adoption rates across sectors in Asia may increase with corporates using the GDPR compliance process to strengthen their key cyber risk practices.[22]

Key reasons cited by firms who have no plans to purchase cyber insurance:

"Cyber insurance does not provide adequate coverage for the cost"

"Cyber coverage is included in another policy"

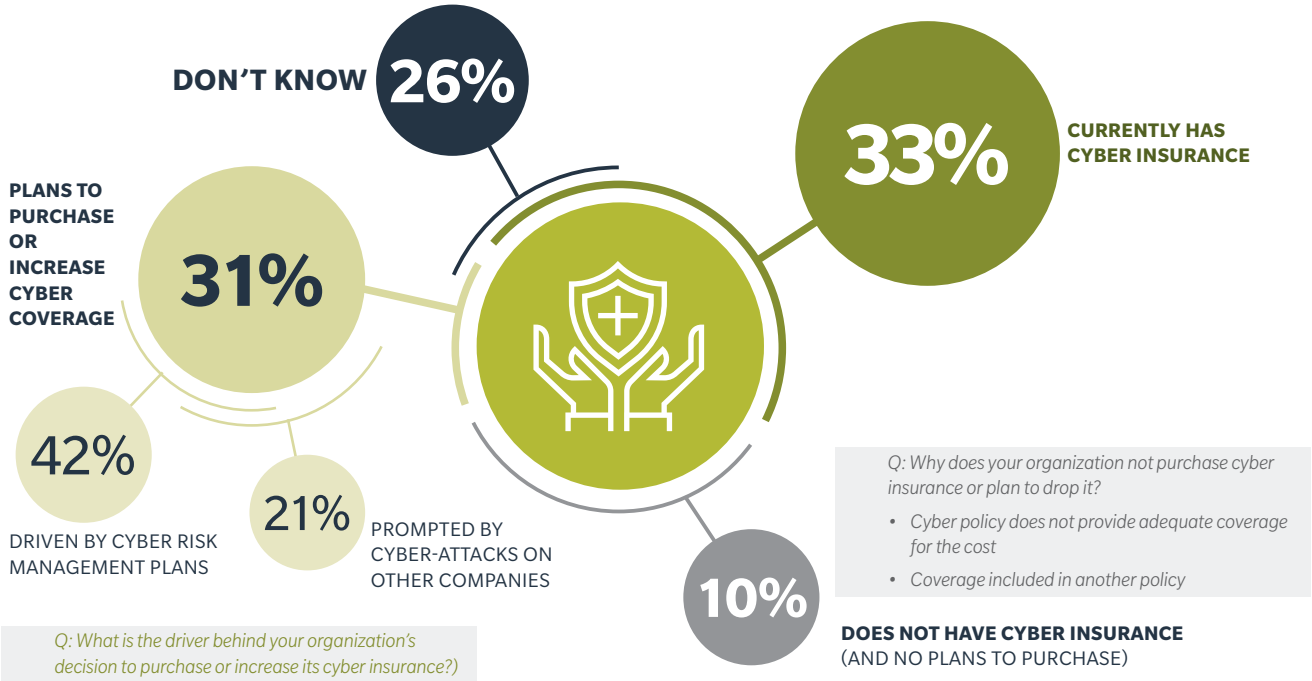
[20] Watering hole attacks are a variant of pivot attacks, in which an attacker is able to pivot from one system (the initial victim usually with weaker security) to another system (the intended target typically with more robust security).

[21] Marsh & McLennan Companies, 2017. Cyber Risk in Asia-Pacific – The Case of Transparency.

[22] Marsh, 2017. GDPR Preparedness: An indicator of cyber risk management. In partnership with Microsoft

EXHIBIT 11: CYBER INSURANCE ADOPTION RATES IN THE RE&H SECTOR IN ASIA
Sources: APRC analysis; dataset from Marsh Hong Kong and Marsh/Microsoft cyber surveys

Q: What is your organization's status with regard to cyber insurance



Q: What is the driver behind your organization's decision to purchase or increase its cyber insurance?)

Q: Why does your organization not purchase cyber insurance or plan to drop it?

- *Cyber policy does not provide adequate coverage for the cost*
- *Coverage included in another policy*

GETTING **CYBER READY**

Identifying the vulnerability of key entry points and taking preliminary steps to strengthen internal cyber defense are crucial first steps to achieving cyber resilience

Identifying the vulnerability of key entry points and taking preliminary steps to strengthen internal cyber defense are crucial first steps to achieving cyber resilience. As revealed by the Marsh cyber surveys, the RE&H sector in Asia has much to lose from a cyber-attack. Respondents' biggest concerns are reputational damage to their organization in the event of a cyber-attack (64 percent), the breach of customer information (55 percent), and business interruption (52 percent). In fact, these indirect expenses in turn will lead to far greater costs in the form of the direct spend required on cybersecurity solutions and post-incident forensics investigations.

The level of cybersecurity maturity of most RE&H organizations in Asia, as suggested by the surveys, is presented alongside the recommended cybersecurity framework that is adapted from the National Institute of Standards and Technology (Exhibit 12).

Cyber risk management is an ongoing process that goes beyond preparing and preventing cyber-attacks. More needs to be done proactively and continuously within the RE&H sector in terms of detecting, responding and recovering from the evolving risk. The gap analysis in Exhibit 13 reveals several actions along the key functions of the cybersecurity framework that RE&H firms can take to strengthen their cybersecurity posture.

EXHIBIT 12: KEY FUNCTIONS OF THE CYBERSECURITY FRAMEWORK AND RECOMMENDED ACTIONS
Sources: APRC analysis; Marsh Cyber Surveys dataset

EXHIBIT 13: GAP ANALYSIS OF THE CYBERSECURITY FRAMEWORK IN THE RE&H SECTOR IN ASIA
Source: Oliver Wyman, APRC analysis

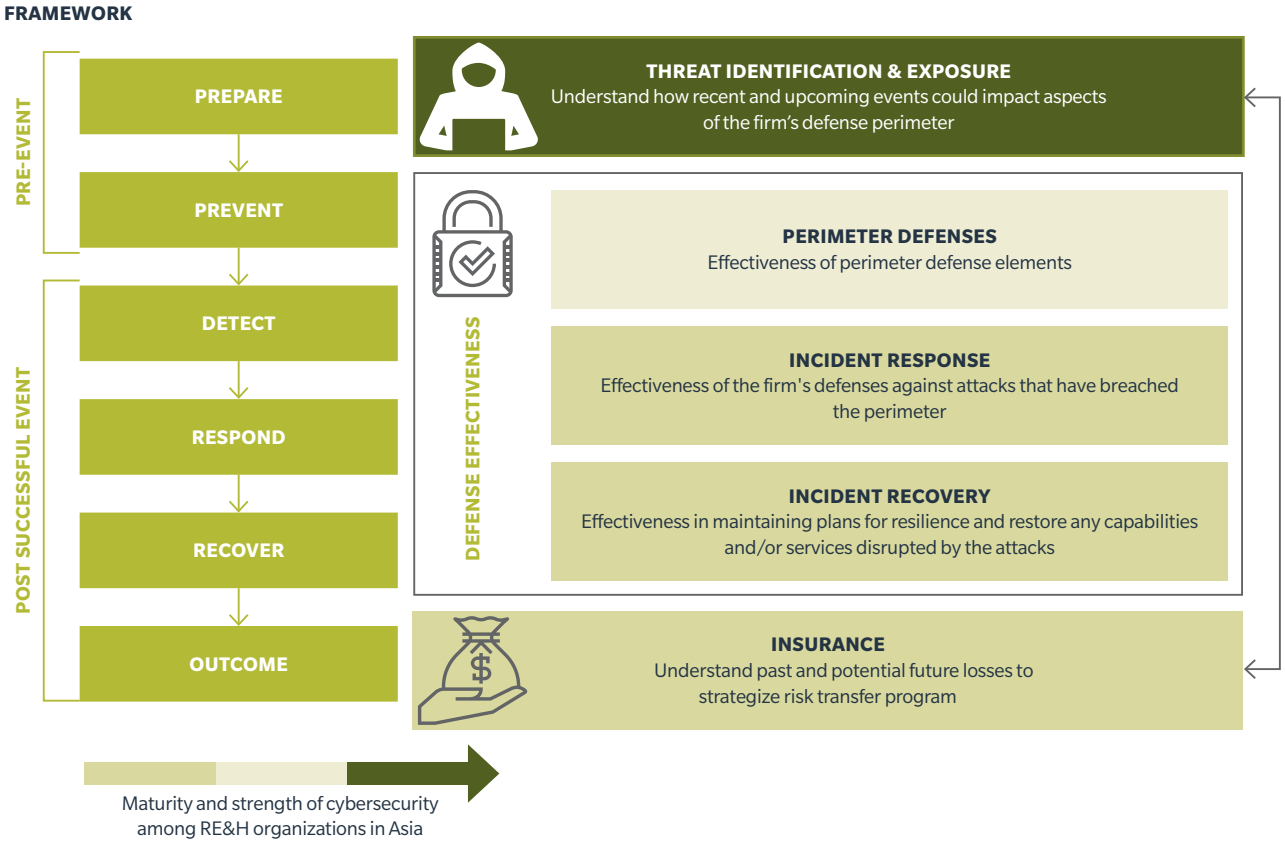
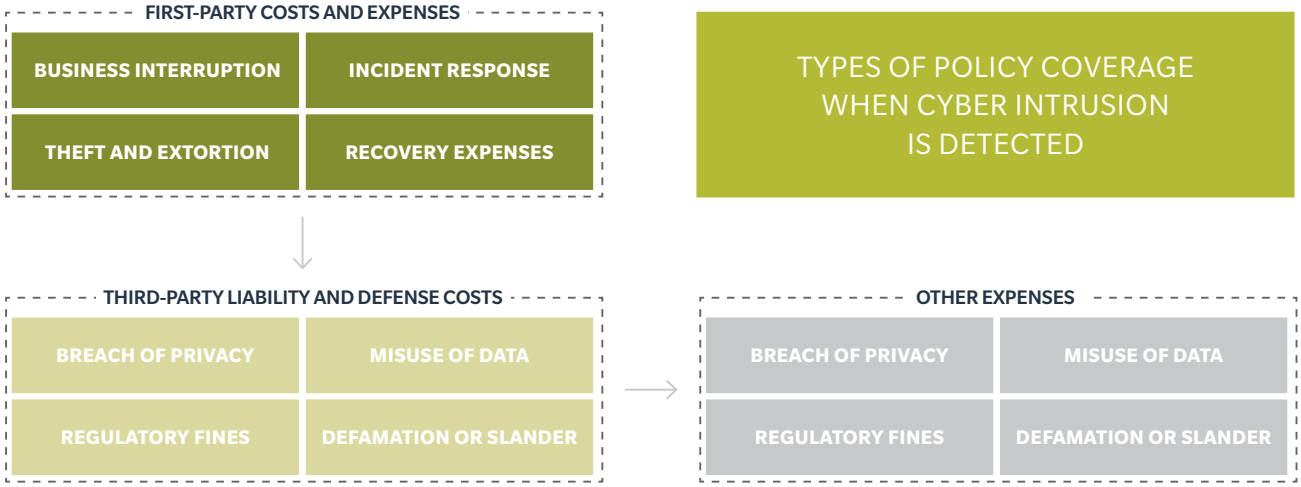


EXHIBIT 14: CYBER INSURANCE POLICY TERMS AND CONDITIONS



Organizations are encouraged to better understand the return on risk, and build in-house capabilities across multiple interconnected functional areas aligned with their cyber strategy.

Our surveys have shown that the level of maturity in threat identification and exposure is high within the sector, while companies have recognized the vulnerabilities of various entry points relevant to their sector. However, cybersecurity defense strategies can be broadened beyond encryption and employee-training programs.

EMBED CYBER IN ENTERPRISE RISK MANAGEMENT PLANS

Enterprise-wide cyber risk management is not commonly accepted; the IT departments are the primary owners and decision-makers for cyber risk management across RE&H firms in Asia, according to the survey results. Often, cyber risks appear as an add-on, outside of holistic risk management with common approaches to segment the risks into financial, strategic, and/ or operational risks.

In order to take on a more proactive approach to enhance cybersecurity, organizations are encouraged to better understand the return on risk, and build in-house capabilities across multiple interconnected functional areas aligned with their cyber strategy. For instance, a top-down approach to set out a cyber risk appetite—the risk that the organization is willing to accept so as to size up mitigation measures—is a first step to recognizing that cyber is an enterprise-wide risk.

STRENGTHEN CYBER-SECURE CULTURE

With cyber-attacks growing in complexity and frequency, there is also an increasing focus on building the foundational processes. The need to shift from a dominant cyber protection strategy to one of risk management discipline equally requires a bottom-up approach, such as creating a more cyber-savvy workforce and strengthening a culture of cybersecurity (such as data privacy, information security, cyber awareness, and accountability) to strengthen the cybersecurity posture. Given that many successful and/or attempted cyber incidents have been attributed to human error factors, it is clear that building effective cyber resilience will have its roots within the culture and its people even with state-of-the-art technologies and strategies.

For example, incident response and recovery are key missing elements that RE&H companies need to urgently build and enhance. Studies have shown that incident response teams and business continuity management are among the top factors capable of reducing the cost of a data breach. [23]

TRANSFER RESIDUAL RISKS THAT CANNOT BE ELIMINATED

It should also be noted that cyber risks cannot fully be eliminated even with the most air-tight cybersecurity measures in place. As such, cyber insurance is another mitigation tool that can transfer some of this residual risk to the insurance and capital markets (Exhibit 14).

[23] Ponemon Institute, 2017. 2017 Cost of Data Breach Study – Global Overview.

CONCLUDING REMARKS

Organizations in the RE&H sector in Asia are more susceptible to cyber-attacks now than ever before. Despite the real estate sector traditionally regarding itself as an unattractive target for hackers, key trends in the region suggest that the real estate, as well as the hospitality sector, are increasingly exposed to cyber vulnerabilities.

Amidst the growing threat, RE&H organizations in Asia are not quite prepared, leading to inadequate cybersecurity defense—they lack key frameworks and mechanisms to prevent and respond to a cyber-attack. Additionally, many of these companies are taking a passive approach towards purchasing cyber insurance, further compounding matters. In fact, many organizations expect to be sufficiently covered under an all-risk policy as opposed to a standalone cyber insurance plan. This approach will need to change sooner than later as attack sophistication grows and regulations mature in the region.

While RE&H organizations embrace new opportunities and efficiency streams that emerging technologies can bring, it is crucial that they recognize the significant risks these opportunities can present. Organizations that develop rigorous programs to prepare, prevent, detect, respond, and recover from cyber-attacks will gain a huge competitive edge over their less-prepared peers, and are more likely to reap higher returns in the longer run.

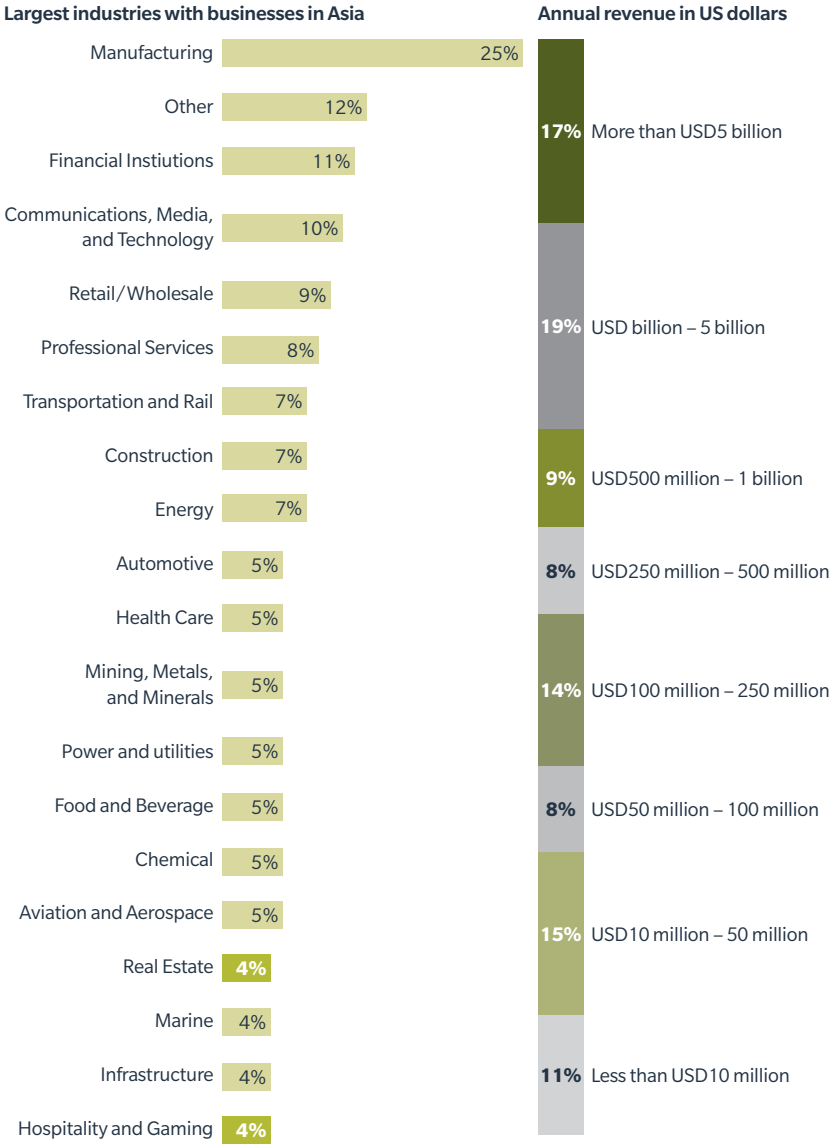
METHODOLOGY

This report is based on findings from the Marsh/Microsoft Global Cyber Risk Perception Survey administered between July and August 2017, as well as the Marsh Cyber Survey for the real estate and hospitality sectors in Hong Kong administered between August and September 2017.

Overall, more than 1,300 senior executives participated in both surveys, representing a wide range of key functions, including information technology, risk management, finance, legal/ compliance, senior management, and boards of directors.

Of all surveyed respondents, 37 percent are from organizations identified with businesses in Asia representing more than 25 industries. Of the 490 respondents at organizations with businesses in Asia, 42 organizations are in the real estate and hospitality sectors, with at least $10 million in annual revenue.

The demographics of both surveys are combined in the statistics below:



BRINK ASIA

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

To read the digital version of Cyber Risk in Asia: Ramifications for Real Estate and Hospitality, please visit **www.mmc.com/asia-pacific-risk-center.html**

Authors

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

MEGHNA BASU
Research Analyst, APRC
meghna.basu@mmc.com

Marsh & McLennan Companies Contributors

Asia Pacific Risk Center: Wolfram Hedrich; **Marsh:** James Addington-Smith, Michael Lewis, Richard Green, Douglas Ure; **Mercer:** Godelieve van Dooren; **Oliver Wyman:** Abhimanyu Bhuchar; **Guy Carpenter:** Michael Owen

The design work for this report was led by Jennifer Cridland, Jesus Pagsanjan, and Mauricio Maldonado, Marsh.

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 addresses the major threats facing industries, governments, and societies in the Asia Pacific Region and serves as the regional hub for our Global Risk Center. Our research staff in Singapore draws on the resources of Marsh, Guy Carpenter, Mercer, Oliver Wyman, and leading independent research partners around the world. We gather leaders from different sectors around critical challenges to stimulate new thinking and solutions vital to Asian markets. Our digital news service, BRINK Asia, keeps decision makers current on developing risk issues in the region.

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

MARSH & McLENNAN COMPANIES