MARSH & McLENNAN COMPANIES | Asia Pacific Risk Center

Managing Your Cyber Risk Posture: From Risk Transfers to Business Continuity Management

MARSH

Authored by:

Jaclyn Yeo
Senior Research Analyst,
Asia Pacific Risk Center

With contributions from:

Richard Green
Managing Director
and Head of Financial
Risk Products, Marsh Asia

Lim Sek Seong
Vice President, Marsh Risk Consulting

UNDERSTANDING CYBER INSURANCE OPPORTUNITIES IN ASIA

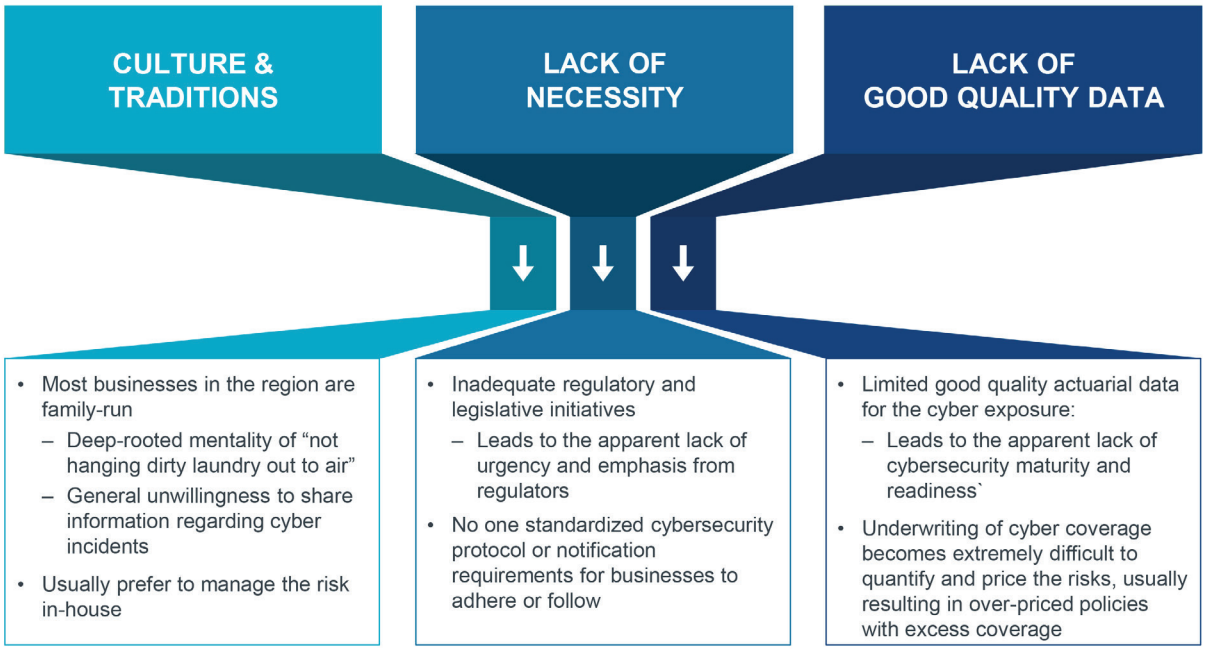
Asia is 80 percent more likely to be targeted by hackers than the rest of the world.[1] However, the relatively higher cyber threat level in Asia is misaligned with the weaker cyber risk mitigation efforts, such as lower levels of awareness, insufficient cybersecurity investments or inadequate cyber insurance offerings. One area where this may be evident is in the low take-up rates for cyber insurance with take-up rates in Singapore (<10 percent) and in Australia (14 percent) significantly lower than in Europe (30 – 36 percent) and the US (55 percent).[2]

The low cyber insurance adoption rates in Asia can be attributed to the general lack of awareness, where the sale of cyber insurance in this region may be influenced by cultural factors and shaped by the current legislative landscape, leading to insufficient data (*Figure 1*) for more accurate pricing of cyber risk.

Limited information and disclosure on the scale and frequency of cyber-attacks in the region may contribute to a false sense of security that could cost businesses. Businesses should not be drawn into a false sense of security and must take actions to prevent and mitigate cyber-attacks by applying the right resources and developing strategic contingency plans to effectively respond when an attack occurs.

First, we realign the common misconceptions businesses may have regarding cyber risk insurance,[3] and provide alternative perspectives to cyber risk transfers. Next, we suggest putting in place best practices in cyber-defence, which include effective endpoint security and IT infrastructure, followed by using cyber insurance to manage the costs of remediation once an incident has occurred. Further, to truly ensure cyber resilience in the organization, businesses are strongly encouraged to further consider putting in place crisis management, business continuity and ICT[4] disaster recovery plans. This is to ensure critical business activities, including the critical ICT application systems and databases, are recovered and resumed. This will minimize operational and business interruptions.

FIGURE 1 KEY REASONS FOR LOW CYBER INSURANCE ADOPTION RATES IN ASIA-PACIFIC



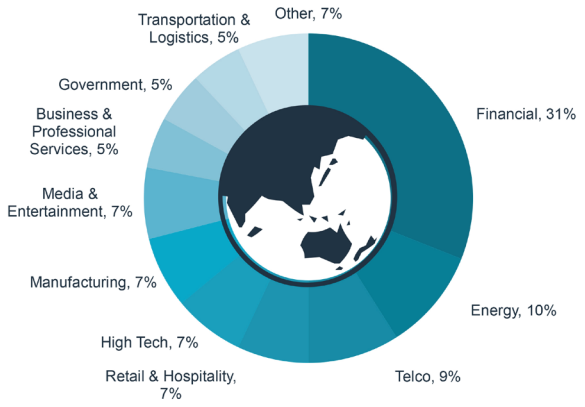
BREAKING DOWN FIVE MYTHS ON CYBER EXPOSURE AND CYBER INSURANCE

"WE DON'T HAVE AN EXPOSURE."

Many organizations have responded that they are able to limit their exposures to cyber vulnerabilities; therefore cyber insurance is not necessary.

However, organizations should be mindful that even employees can represent a privacy exposure – the data storage of employees, retired employees, and dependents of employees may be compromised, resulting in a privacy data breach. In fact, any organization that uses computers or mobile devices connected to the network is potentially exposed. Even though organizations outsource their employee data management function, the exposure and liability remain with the organizations as they have the legal obligation to protect it.

FIGURE 2 2017 LIKELIHOOD OF INDUSTRIES BEING A TARGET FOR CYBERCRIMES IN ASIA-PACIFIC[5]



***Others** Include: Biotech & Pharmaceuticals, Healthcare, Construction & Engineering, And Non-profit*

According to recent investigations carried out by FireEye iSight Intelligence,[6] while the financial services (31 percent) record the largest risk, all other sectors are almost equally at risk (5 – 10 percent) of being targeted for cybercrimes in the Asia-Pacific region *(Figure 2)*.

For example, cyber-criminals can attack organizations' core systems through the point of sale for a retailer, the billing systems for an insurance company, the information processing systems at a financial institution, or the automated machine lines at a manufacturer. Regardless of sector, cyber-attacks can lead to severe disruption of daily operations and business processes, supply chain and vendor communication issues, as well as loss of revenues and reputational damage.

With an ever-evolving cyber risk landscape, the exposure has since extended beyond data privacy into network security systems; thus disruptions to both network security and daily operations can have severe financial impacts on businesses, and bottom lines in particular.

"IT'S TOO EXPENSIVE/ NOT IN THE BUDGET TO BUY CYBER INSURANCE."

Cyber insurance coverage can potentially be expensive; however, the real question that business leaders truly ought to ask is whether the cyber insurance coverage they are presented with is adequate to meet their specific needs. There may be instances where the risk quantification and pricing processes

[1]See http://www.bbc.com/news/technology-37163076

[2]Cyber risk in Asia Pacific: The case for greater transparency, MMC Asia-Pacific Risk Center, 2017

[3]These are some common remarks and feedback comments gathered in Asia by Marsh, the global insurance broking and risk management firm

[4]ICT is the abbreviation for information and communications technology

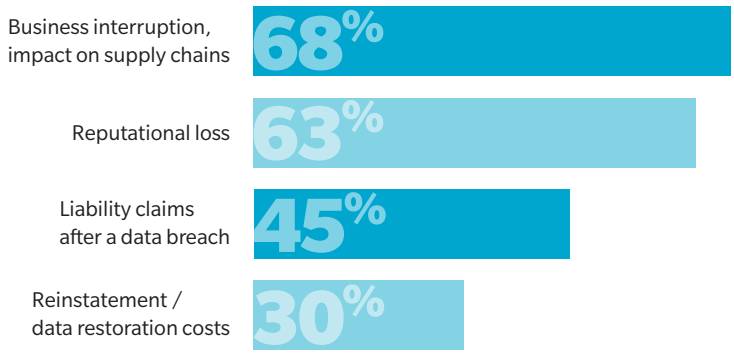
[5]The investigation uses an intelligence-led approach to measure industries' cyber threat profile, which is a proxy for the likelihood of the industry being a target for cybercrimes

[6]M-Trends 2017: A view from the front lines. Mandiant-FireEye, Mar 2017

are too conservative due to the lack of good quality actuarial data for the cyber exposure, leading to excess coverage and over-priced cyber policies. The perception that cyber insurance is too expensive and not within the budgets of many can be easily addressed if the organizations engage independent risk specialists to advise and broker a comprehensive yet reasonably-priced cyber insurance coverage suited specifically to their needs.

Another cost angle that organizations should consider is the financial impacts in the event of a cyber-incident. Business interruption (BI) impact, the main cause of economic loss after a cyber-incident, is the cyber concern companies worry most about, according to the Allianz Risk Barometer Report 2017 *(Figure 3)*. Estimates of BI costs range between $1 – 4 billion[7] as companies shut down their operating systems, reformat computers and servers, and recover critical data from backup units. Hence, transferring some of the risks to insurance and capital markets may be relatively more cost effective as compared to absorbing all direct and indirect costs incurred during a cyber-incident.

FIGURE 3 MAIN CAUSES OF ECONOMIC LOSS FOLLOWING A CYBER-INCIDENT[8]
Sources: Allianz Risk Barometer Report 2017



Cyber Business Interruption Quantification is an approach that enables organizations to determine and prioritize cyber risk scenarios based on the potential financial impact. Cyber risk scenarios and/or cybersecurity control measures are identified and evaluated. Using a combination of pre-loss business interruption analysis and analytics modeling, the qualitative impacts are assessed and quantitative impacts further evaluated. This measurable outcome enables organizations to prioritize and allocate valuable funds and resources to mitigate the high-impact risk scenarios.

The more efficient and effective use of equity addresses key cost concerns of business leaders, where cyber insurance coverage becomes relatively inexpensive when compared to the likely cost of an attack.

"OUR IT TEAM HAS OUR CYBER RISK UNDER CONTROL."

IT departments continue to take primary responsibility for cyber risks in the majority (56 percent) of smaller organizations in the UK, while board-ownership of cyber risks exists in less than 20 percent of the organizations surveyed.[9]

IT engagement is an important part of addressing the total cyber risk to an organization, but in today's marketplace, cybersecurity is no longer just an IT-department issue. It is an enterprise risk issue that must be considered and addressed by the many stakeholders throughout the organization, amidst an ever-changing environment of cyber threats.

Accidental breaches, employee exposures, and malicious hackers are just among the many unique ways businesses can be exploited, such that if the organization only focuses on direct external cyber risks, it most probably will miss a significant portion of its total exposure.

Asia is also becoming a growth area for litigations; organizations are facing increasingly complex network and security issues as well as lawsuits and reputational damages, which broaden the spectrum of risks and increase the potential losses that organizations and board members face in their daily operations.

[7]See http://insuranceasianews.com/countries/china/wanncry-hit-asia-hard-but-wont-boost-cyber-policies/

[8]Allianz Risk Barometer Top Business Risks 2017, Allianz 2017

[9]UK 2015 Cyber Risk Survey Report, Marsh June 2015

"THIS IS ONLY A BIG COMPANY PROBLEM."

It is also seen that bigger corporations are often associated with headline grabbing cybersecurity incidents; however recent studies have suggested that watering hole attacks on small- and mid-sized enterprises (SMEs) are becoming increasingly popular.

Small data grabs are harder to detect and prevent, hence the compromised information often appears more valuable in the black market. Further, SMEs have fewer resources devoted to cybersecurity infrastructure and are perceived as easier targets for cyber criminals to exploit to gain access into the networks of bigger organizations.

Therefore, data breaches are as much a Main Street concern as a Wall Street issue. More than half of surveyed SMEs in the UK (57 percent) viewed internal threats and operational human error (such as loss of mobile devices) as the greatest threat to their organizations,[9] which re-emphasizes cyber is as severe a problem for SMEs as well.

Regardless of the organizations' size, the threat level remains the same, and it depends heavily on individual organizations to limit their exposure and mitigate their cyber vulnerabilities.

"WE BUY A LOT OF INSURANCE POLICIES; IT HAS TO BE COVERED UNDER ONE OF THEM, RIGHT?"

The ever-growing and ever-evolving cyber risks have uncovered various gaps across many traditional forms of insurance, rendering them inadequate to respond quickly to these cyber exposures.

There may be some elements of cyber coverage in General Liability (GL) and Professional Indemnity (PI), but neither is specifically underwritten to respond to a cyber-breach incident. Moreover, these policies usually have specific exclusions that omit accidental coverage for a data breach incident. Even if that insurance claim is triggered, it does not cover data breach response costs.

For example, GL policies do not provide coverage for damage to electronic data, criminal or intentional acts of insureds or its employees, or any pre-claim expenses (such as notification costs and regulatory defense). PI policies also often limit coverage to claims arising from negligence in performing specifically-defined services and exclude coverage for criminal acts of insureds or their employees, and first party loss expenses associated with a privacy breach or cyber-attack.

THREE-PRONGED APPROACH TO ENHANCE CYBER RESILIENCE

Cyber risk should be recognized as an enterprise-wide risk, and cyber insurance should be supplemented with endpoint security measures and business continuity plans to build and enhance cyber resilience into the organization. A more detailed action plan is presented here to demonstrate a three-pronged approach for companies *(Figure 4)* to consider in moving towards a greater focus on cyber resilience.

FIGURE 4 A BALANCING ACT OF KEY COMPONENTS TO ENHANCE CYBER RESILIENCE

1. EFFECTIVE ENDPOINT SECURITY MANAGEMENT

Endpoint security responses, which include threat detection and prevention, are usually the first line of defence against cyber-attacks, and for organizations that are compromised in the event of a cyber-incident, the first response – the easiest and the cheapest way – is to protect themselves using legitimate software and keeping endpoint security up to date.

Hence endpoint security entails following a definite level of compliance to standards for the protection of computer networks and individual devices, which are commonly used as entry points into corporate networks. Endpoints are often defined as end-user devices, laptops, desktop PCs, as well as hardware such as servers in data centres. Endpoint security addresses the risks presented by devices connected to an enterprise network.

Endpoint security features typically include a secure foundation for IT processes and infrastructure, anti-virus software, firewalls, email encryptions, and regular backups onto servers that are disconnected from the cloud. As cyber threats continue to evolve and increase in frequency and severity, upgrades have been made to traditional endpoint security, making it smarter and moving beyond prevention.[10]

For example, threat intelligence for multiple detection and prevention protocols is gaining traction, from detection and investigation to remediation and recovery. Further, with greater interconnectivity and increasing complexity within organizations as we move towards digital transformation, the key attribute of scalability to detect and prevent threats enhances the capacity of operation system support.

2. LEVERAGE ON RISK TRANSFER

Insurance is one of the many essential tools in the risk mitigation toolbox. Although it is clear that a cyber-policy cannot fully shield an organization from cyber breaches, as much as an insurance coverage does not completely eliminate the risk, it is essential to note that it can keep organizations on stable financial footing should a significant security event occur.

As illustrated earlier, cyber insurance is one key component to enhance cyber resilience, as it transfers some of the risks to the insurance and capital markets and offsets some of the costs.

The necessary step to implement this component is to first educate and nurture businesses, so as to engage in deeper and more meaningful cyber conversations. Businesses need to be aware of the potential impacts cyber threats may bring about as well as the reassurances from suitable

[10]FireEye discusses the next-generation endpoint security at the "Smarter Endpoint Security: How to go beyond Prevention" live Webinar, June 2017

policies, before they will perceive cyber insurance as a necessary risk-management strategy for their organizations.

In terms of the coverage components, cyber policies provide reimbursements for the fees, expenses and legal costs associated with cyber breaches that occur after an organization has been compromised or loss of confidential information. Besides first party costs and expenses (such as business interruption) as well as third party liability and defence costs (such as litigation, regulatory fines and penalties), other expenses that can be covered under cyber policies include forensic investigations, data recovery, and public relations, among others.

Essentially, risk transfer through cyber policies will allow organizations to protect themselves against unexpected losses due to cyber-incidents that can otherwise drive up the cost of operations, destabilize the organizations' cash-flows, and weaken shareholders' confidence. Cyber insurance presents a more effective and efficient use of equity while protecting the financial earnings of businesses.

3. MAKE BUSINESS CONTINUITY MANAGEMENT PLANS

Business Continuity Management (BCM) is an all-inclusive process that enables organizations to better prepare in advance for, and respond to, potential crises situations that may lead to business interruptions. The main objective of BCM in this context is to put in place Business Continuity Plans (BCPs) to ensure the continuation of critical functions in the event of a cyber-attack crisis. This is then followed by conducting fire drill exercises to familiarize the organizations with processes involved to effectively execute the BCPs should the need arise. Finally, as part of the ongoing process of BCM, these BCPs will require regular stress-testing and updating so as to improve the efficiency and effectiveness to continuously adapt and mitigate the ever-evolving cyber threats.

Despite, there may be concerns from businesses that they have already planned for data recovery and post forensic investigations in response to cyber-incidents; hence cyber BCM is neither necessary nor required. However, such forensic investigations and post-incident responses do not necessarily ensure that critical functions of the business will recover and resume on time. Further, not all business and operational functions are equally critical to render systems recovery all at once. Therefore, it is imperative for businesses to identify and determine the criticality of each business function and each ICT application, databases and service, so as to ensure the resources are utilized effectively for prompt recovery of key functions.

FIGURE 5 POSSIBLE PATHWAYS OF EFFECTIVE BCM IN ACTION

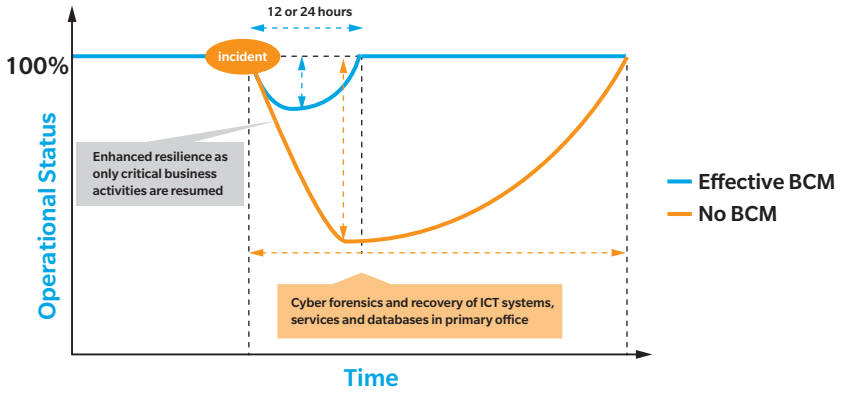


Figure 5 illustrates the potential operating pathways (operational status and recovery periods) – of organizations challenged with cyber adversaries that lead to business interruptions – with or without effective BCM put in place.

While it may take two weeks or longer for post-incident forensic investigations and recovery of the primary ICT systems, services and databases in the primary office, organizations can activate the BCPs and resume critical business activities within 24 hours, depending on the criticality of the business functions. On the other hand, functions and ICT application systems, services and databases that are deemed not critical during the cyber-attacks, may be temporarily suspended.

With the appropriate focus of financial and essential resources on critical areas to develop an effective BCM, which includes data protection, loss prevention backup solutions, and ICT disaster recovery plans (DRPs), huge economic losses as a result of business interruption in the event of a cyberattack can altogether be avoided, or at least minimized.

WHAT IF DATABASES FOR DISASTER RECOVERY ARE ALSO INFECTED?

There have been instances where databases required for DRPs may potentially be infected with malware or ransomware. In situations like this where the ICT environment replicates data from the primary system to the secondary system, and the infection spreads across critical functions, it becomes clear that the traditional strategy of backing up to an offline storage medium (such as endpoint security) remains necessary such that a backup copy of the data remains intact. Therefore, databases required for the DRPs may be recovered without significant concerns about whether the data is reliable after being recovered through cyber forensics.

EVOLVING WITH THE RISKS AND UNCERTAINTIES AHEAD

We believe that cyber resilience of most organizations can be enhanced via this three-pronged approach – proper and up-to-date endpoint security, cyber insurance, and effective BCM – thereby reducing the significant costs and recovery downtime to business interruption.

Business leaders ought to focus on finding the right balance between cybersecurity investments in endpoint security management and BCP, as well as securing the appropriate cyber insurance coverage suitable to the relevant and unique needs of their industry and organization.

It is critical for organizations to continuously assess and improve the understanding of their cyber risk posture, so as to make strategic decisions around the business operations, develop cyber resilience, and better prepare for the uncertainties in an increasingly digitized world.

About Marsh

Marsh is a global leader in insurance broking and risk management. Marsh helps clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. Marsh's approximately 30,000 colleagues work together to serve clients in more than 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. With annual revenue of US$13 billion and more than 60,000 colleagues worldwide, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a leader in providing risk and reinsurance intermediary services; Mercer, a leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a leader in management consulting. Follow Marsh on Twitter @MarshGlobal, or on LinkedIn, Facebook, and YouTube.

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.