StrategicRISK

CYBER RISK

Risk managers voice their reservations about cyber risk, from safeguarding client data to cyber insurance frameworks

In association with

AIG®

What's holding cyber insurance back?

Risk managers are keen to mitigate their cyber exposures, but have reservations about the insurance policies available to them

When it comes to adoption by risk managers, cyber insurance seems to be at a tipping point. Of the 200-plus delegates at the 2016 Strategic Risk Forum in Singapore, only 23% had a standalone cyber liability policy, but more than one-third were considering a purchase. So, is something causing a disparity between demand and adoption?

MITIGATING CYBER EXPOSURES

Andrew Mahony, regional director, Financial Services & Professions Group, Aon, says cyber losses – caused by malicious attack, user error or both – are unavoidable. "Companies with good governance and security measures can reduce the likelihood or limit the impact of these losses, but the threat cannot be eliminated," he adds.

"For that reason, cyber risk transfer needs to be considered in conjunction with risk prevention. Cyber insurance enables companies that prioritise cyber security to implement a holistic response to their cyber exposure."

Aon's clients first seek to understand their cyber risk profile and how their existing insurance programme addresses cyber exposure, says Mahony. "When gaps emerge in that analysis, companies look to cyber insurance to cover their exposure. The primary concern for most companies is the large amount of sensitive data for which they are responsible – for customers and employees – although the potential for operations to be shut down by a cyber attack is also a significant risk.

"Companies are also looking to insurers to provide direction and expertise with the engagement of external consultants to assist in cyber remediation actions."

WEIGHING THE PROS AND CONS

As cyber insurance matures as an offering, it is boosted by its benefits and restricted by its issues.

"INSURERS AND BROKERS NEED TO GET BETTER AT COMMUNICATING TO IT SECURITY PROFESSIONALS, AS WELL AS INSURANCE BUYERS AND RISK MANAGERS, IN RELATION TO HOW CYBER INSURANCE PRODUCTS CAN COMPLEMENT A FIRM'S EXISTING RISK MANAGEMENT REGIME AND MITIGATION FRAMEWORK"

Risk financing lead, EnergyAustralia
Richard Cassidy

On the positive side, Mahony says cyber insurance offers well-rounded cover for both the direct loss suffered by a company and its liability to third parties.

"Good cyber insurance policies provide cover for business interruption, regulatory fines and penalties, and cyber extortion events," he says. "Pricing in the Asian market, while not yet consistent, is far more competitive than in other markets."

AIG Singapore head of financial lines Lai Yen Yen adds: "Comprehensive insurance cover can help a company get on the front foot as soon as a breach has taken place, by deploying a cyber security response team to offer immediate and professional counsel for

legal, public relations and auditing matters."

Geetha Kanagasingam, vice-president for UK, Europe & APAC, Group Insurance and Group Risk, Barclays Bank, says cyber insurance also provides the scope that covers data breach notification expenses. For many regulators, this is now a mandatory requirement. "[Cyber insurance also] fills up the gaps of cover, as only some aspects of the cyber coverage elements may be found in existing policies such as crime policy and/or professional indemnity."

Kanagasingam says cyber insurance may also offer a competitive edge, as more clients are asking whether firms have such a policy in place.

A general drawback, says Mahony, is the absence of cover for bodily injury and property damage arising from cyber events, under both traditional insurance products and cyber policies.

Kanagasingam adds that there is still insufficient capacity in the cyber insurance market: "[The] limit purchased may range from single digit in millions to triple digits in millions globally, notwithstanding the fact that the demand for higher limits is increasing."

There are additional costs too, she says. Premiums are volatile "since this is a fairly new insurance product with relatively young history of data".

Other issues stem from the need for extensive disclosure, says Kanagasingam. Insurers tend to request sensitive, confidential, internal information. "Are firms confident to reveal this information to insurers who, after all, are also potential targets to cyber risk events?" she asks.

RISK MANAGER CONCERNS

Cyber exposures have piqued risk managers' interest in cyber insurance products, but several concerns have dampened their adoption rates.

"We have made some initial [cyber insurance] inquiries," says Richard Cassidy, risk financing lead, EnergyAustralia, "and obtained premium indications for an 'off the shelf ' product, but did not proceed to a purchase."

Cassidy says that while cyber insurance offerings address many of the potential cyber exposures, gaps remain. "Insurers and brokers need to get better at communicating to IT security professionals, as well as insurance buyers and risk managers, in relation to how cyber insurance products can complement a firm's existing risk management regime and mitigation framework," he adds.

Another risk manager told *StrategicRISK Asia* that despite shopping around, they have not purchased cyber insurance, "due to low limits and very narrow wording". The risk manager believes this is due to the "immaturity of the product offering to date".

"Cyber insurance has not been, and I doubt ever will, get to the real pain points which companies face in this space, such as cover for 'loss of opportunity' if, for example, there is a known cyber intrusion which accesses confidential bid information, which then subsequently means the bid is lost," he says.

Barclays' Kanagasingam adds that, as such gaps persist in cyber insurance, it remains the case that such cover is no replacement for a robust cyber prevention and security programme.

Safeguarding clients' data is paramount

Cyber criminals see customer information as a goldmine

The loss of customer data is the main cyber risk facing most companies, but keeping their IT systems up to date would be the first step in mitigating the risk.

Asked to identify the cyber risk that worries them most, the majority of delegates (37%) at the 2016 Strategic Risk Forum in Singapore cited the loss of customer data (see graph below).

According to David Siah, country manager, Singapore at Trend Micro, this is not surprising.

"Some customer records are more expensive on the black market than credit card data, because credit cards can be disabled, but a personal record follows you for life. A key example would be a medical record. Once a hacker gains access to that information, they can use it for a lot of other purposes throughout a person's lifetime," he explained.

Willis Towers Watson Singapore Finex leader Frances Fu concurred.

"We have a lot of dialogue with customers about cyber insurance – whether it covers regulatory fines, crisis management, forensic costs and so on, especially when personal identifiable information of their customers is compromised," she said.

"SOME CUSTOMER RECORDS ARE MORE EXPENSIVE ON THE BLACK MARKET THAN CREDIT CARD DATA, BECAUSE CREDIT CARDS CAN BE DISABLED, BUT A PERSONAL RECORD FOLLOWS YOU FOR LIFE."

Singapore country manager, Trend Micro
David Siah

Fu added that cyber insurance does not just cover the costs incurred as a result of the privacy breach, but can also cover the first party and third-party losses.

Another type of cyber attack on the rise in recent years is ransomware, where cyber criminals encrypt data and ask for money to decrypt it.

Siah said: "If you receive an encryption notice on a critical business file, do you pay the ransom or not? Many people do pay … so that's why ransomware has become a very big problem."

He said that most breaches happen because the company has not updated its systems and software, leaving the back door open to hackers.

"Client data is inevitably one of the most important aspects of [our] business," said Geetha Kanagasingam, Barclays vice-president UK, Europe & APAC, group insurance and group risk.

"For cyber risks, Barclays groups its control requirements under four key categories. These are attacks on us, attacks on our customers, attacks on the availability of our services and attacks on critical banking structure. There is no appetite for control gaps rated as critical."

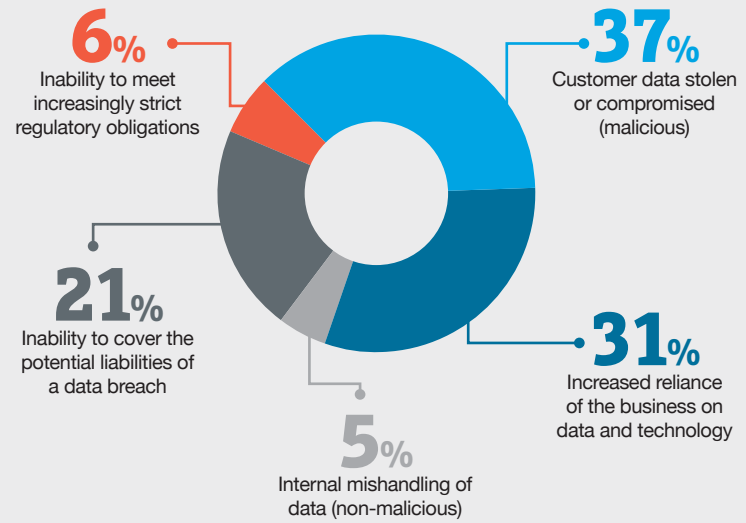
When asked about how best to manage cyber risk, Kanagasingam said: "Implement a robust IT security and cyber risk prevention programme. A chief information security officer should be appointed to be the risk owner who comes up with the policies, the procedures and the programmes, working with the relevant stakeholders within the business.

"Risk managers ought to work closely with the first line of defence that includes the CIO, CTO, COO etc – to provide inputs and possible solutions from a risk and insurance perspective as part of a holistic risk management strategy, creating a second line of defence in preventing and/or mitigating losses."

Christophe Durand, head of cyber strategy at Interpol, said corporates should make intrusion detection their top priority.

"We all know now that it is impossible to get a 100% secure information system, so we should consider the fact that the enemy is within your information system, so you have to monitor the behaviour of your system in order to identify what is going on in your system."

Which cyber risk is the biggest concern for you?



Source: Strategic Risk Forum 2016

Inside the cyber risk model debate

Is a public-private partnership the only way to cover cyber risk?

Sobering estimates of the capacity needed to cover cyber risks in Asia have led many to ask whether the insurance industry is too small to cope.

It may be that the only solution is a public-private partnership, with a pooled scheme backed by the government, as is the case with terrorism and flooding.

Much of the discourse around this comes from Nanyang Technological University (NTU Singapore). Its Cyber Risk Management (CyRiM) Project is designed to help businesses and institutions defend themselves.

Professor Shaun Wang, director of the Insurance Risk and Finance Research Centre (IRFRC) at NTU Singapore's Nanyang Business School, said: "A public-private partnership on cyber risks can help promote awareness and best risk management practices.

"Cyber risk is relatively new, an emerging risk that evolves rapidly. There is a need to collect data and share information among organisations. There are also gaps in terms of definitions of cyber losses and standardisation of insurance policies. These gaps are best addressed through public-private partnerships."

Wang said a realistic goal is cyber resilience, rather than blanket protection covering losses. Potential complications include mixing up roles and creating the wrong incentives. "For instance, if government creates a back-stop or pooled scheme, there may be less incentive for the private sector to carefully monitor their accumulation of risk exposures."

The CyRiM Project is supported by the Monetary Authority of Singapore, Cyber Security Agency of Singapore, and five industry partners: Aon Centre for Innovation and Analytics, Lloyd's, MSIG Insurance, SCOR and TransRe.

Andrew Mahony, regional director, Financial Services & Professions Group, Aon, said: "Government and private enterprise engagement and co-operation is critical to the improvement of cyber security standards and the development of the cyber insurance market."

But FireEye Asia-Pacific chief technology officer Bryce Boland said: "We must be wary of using public funds to pay for the failings of duty of care and diligence in operating private institutions. As with bailing out the banks, we risk privatising the benefits (less investment in data protection and security) and socialising the losses (the public providing cover for security failures)."

"CYBER RISK IS RELATIVELY NEW, AN EMERGING RISK THAT EVOLVES RAPIDLY. THERE IS A NEED TO COLLECT DATA AND SHARE INFORMATION AMONG ORGANISATIONS"

Director, Insurance Risk and Finance Research Centre, NTU Singapore
Professor Shaun Wang

SPONSORED WORD

OUTSOURCING CREATES GREATER RISK OF CYBER EXPOSURES

LAI YEN YEN
Head of Financial Lines, Singapore, AIG

In the current business landscape, companies can ill-afford to ignore cyber risk exposures. A growing number of high-profile cyber attacks against multinational companies (MNCs) have alarmed directors of large companies into protecting themselves and their companies against breaches.

Outsourcing has been thrust into the spotlight as a key area of concern for MNCs. Today, more companies are outsourcing non-core functions to keep themselves competitive and their costs sustainable. In a market update AIG Singapore put out in March 2016, we forecast cyber risks would emerge this year from internal and external factors, including outsourcing to third-party providers.

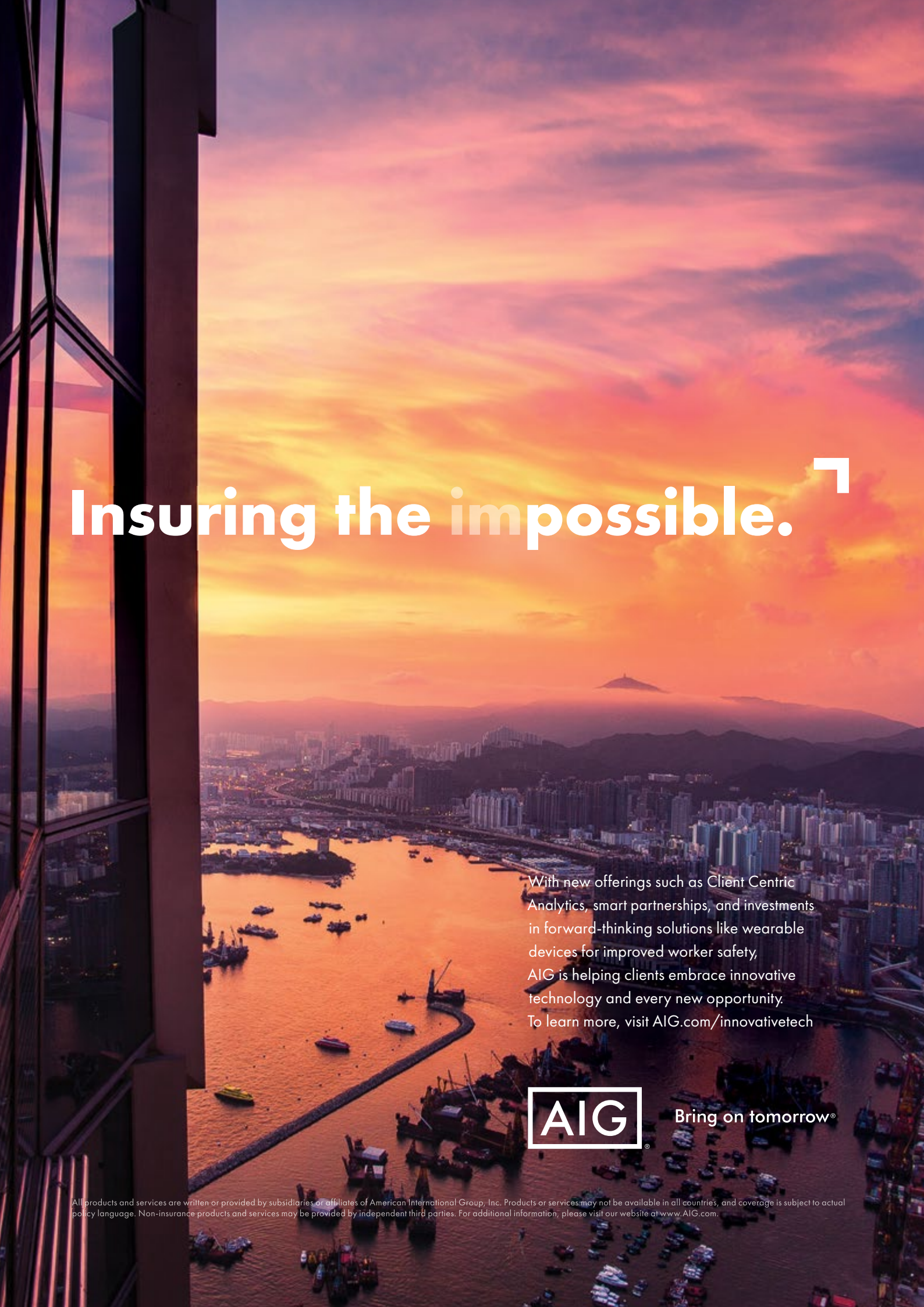
In an environment where MNCs have multiple vendors supporting their business, it is wise to find out the risks these vendors can potentially bring. Should the vendor be faced with a cyber incident, the MNC will likely be similarly impacted by a loss of reputation and consumer confidence.

With greater awareness of such attendant risks, MNCs should ensure their vendors have a robust risk management framework in place against cyber risks, and undertake regular due diligence and continuous monitoring of their vendors. This is especially critical in an environment of continuous technological advancements, where new cyber risks are constantly emerging.

For example, two years ago, bank statements of private banking clients were stolen from the server of the bank's printing vendor. The bank had to deal with ensuing customer complaints and regulatory enquiries, even though it was not directly responsible for the loss of the statements.

Cyber risks affect MNCs, directly or indirectly. A holistic approach to risk management of vendors, including cyber risks, is vital to a successful and trusted partnership as more companies move towards outsourcing arrangements.

› For more information visit www.aig.com.sg/cyber


Insuring the impossible.
With new offerings such as Client Centric Analytics, smart partnerships, and investments in forward-thinking solutions like wearable devices for improved worker safety, AIG is helping clients embrace innovative technology and every new opportunity. To learn more, visit AIG.com/innovativetech
AIG
Bring on tomorrow®
All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. For additional information, please visit our website at www.AIG.com.