StrategicRISK

SPECIAL REPORT:

CYBER CLAIMS

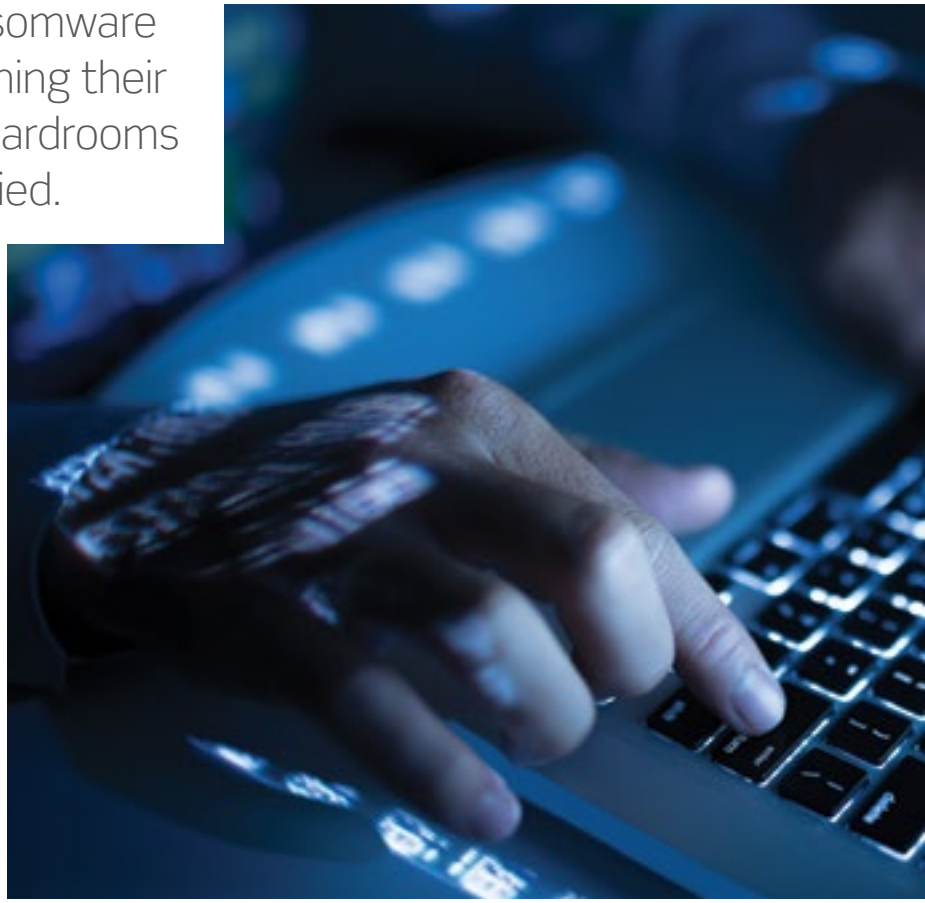
The recent WannaCry ransomware attacks have spurred businesses into bolstering their online defences. But what can we expect from the next generation of cyber threats, and how will the insurance industry respond?

In association with

AIG

How WannaCry shook the world

In the wake of the global ransomware attack, companies are examining their cyber insurance and Asian boardrooms are growing increasingly worried.



Some events are landmarks in the evolution of certain types of risk. When it comes to cyber risk, this certainly applies to WannaCry.

The worldwide cyber attack by a ransomware cryptoworm, which started on Friday, 12 May 2017, targeted the Microsoft Windows operating system. Having encrypted data, it demanded payments in Bitcoin to undo the damage. Within a day, about 36,000 WannaCry attacks were detected across Europe and Asia alone.

In the aftermath, it's clear that the attack highlighted the need for a strong incident response plan and the value of cyber insurance. However, insurers have started to process payouts already.

"The take-up rates with cyber insurance is driven out of the United States," says Richard Green, managing director and head of financial risk products at Marsh Asia. "Many US corporations would buy cyber insurance quite routinely. However, the take-up rate for cyber insurance in Asia is still fairly low. It is a product which is attracting a lot of interest recently, but it is still in its infancy."

FIRST RESPONDERS

What this means, says Green, is that the big cyber insurance claims in this case will not be coming from Asia. He also notes that there is no such thing as a standard cyber insurance policy.

"All of the cyber insurance policies on offer from each of the carriers is slightly different. That said, they do contain some common features," he says. "In terms of claims, the first thing you are going to see under most cyber insurance polices after a ransomware attack is they contain incidence response.

"The incident responders, as the name suggests, go in and see if they can assist clients in identifying the problem and, if possible, fixing the problem."

Another aspect of coverage is the payment of the ransom, he says. "Most cyber insurance policies do provide payment of the ransom costs if a ransom is demanded. We are advised that certain insurance even have Bitcoin accounts set up for that purpose However, in certain jurisdictions, the paying of ransom is not legal."

"THOSE WHO HAVE MOST CONCERNS ARE CLIENTS WITH NO CYBER POLICY WHO ARE TRYING TO FIND OUT IF OTHER POLICIES, SUCH AS LIABILITY OF PROFESSIONAL INDEMNITY, CAN BE CLAIMED AGAINST."

Lockton Wattana Thailand director **Peter Jackson**

Some companies that have paid a ransom have yet to see their data restored, Green adds.

Peter Jackson, director of multi-national clients at Lockton Wattana Thailand, says the substance of WannaCry attack claims is likely to involve first-party costs for managing the situation and any business downtime that resulted in a loss of profits.

"As it was a shotgun-style ransomware attack, it is less likely to have had an impact on customer data and associated third-party liability claims," he says.

While most claims have been under cyber policies, Jackson says crime policies could have been impacted as a result of the ransom. Then again, the amounts in question, perhaps $300-$600, are probably too small to trigger the policy. "If a company has got into serious operational problems, there is a risk of a claim on their

CHINA'S CYBER SECURITY LAW: ARE YOU COMPLIANT?

China's Cyber Security Law (CSL) came into effect on 1 June. Carla Liedtke, director, Control Risks, tackles some of the key questions it poses to multinational companies (MNCs).

Who will be captured by the law?
It is very likely that many MNCs will feel the heat. The brunt of the CSL falls on 'critical information infrastructure' (CII) operators, which includes power, transport and finance, and other infrastructure that could harm 'people's livelihoods'. This means any foreign company that is a key supplier to a 'critical' sector, as well as any company that holds significant amounts of information on Chinese citizens, could be in scope.

What is covered by the law?
There is a particular focus on 'personal information' and 'important data', both of which are vaguely defined. This is significant as network and CII operators will be required to localise this information to China, and a security self-assessment or approval from the relevant regulator will be required before transferring this data abroad.

What are the risks for MNCs?
The sheer scope of the CSL is mind-boggling, and also extremely vague. This means it is currently impossible to be 'compliant' and companies will need to focus on how the CSL will be enforced by regulators. Moreover, the presence of multiple industry regulators will result in patchy interpretation, conflicting signals and unpredictable enforcement.

The CSL potentially provides the government with the legal ability to obtain intellectual property and a view into an organisation's cyber gaps and vulnerabilities. The operational costs and risks of localising data to China are likely to be significant for most MNCs, particularly the loss of the ability to conduct global big data analytics if the China data has to be housed separately. There is also significant risk that foreign technologies that are uncertified under the CSL could be shut out of the China market in order to benefit domestic versions.

D&O policy from regulator or shareholder actions, but this doesn't seem likely at this stage," he adds.

A SILVER LINING?

Jackson says the most common question affected clients are asking is simply: 'Am I covered?'

"Those who have most concerns are clients with no cyber policy who are trying to find out if other policies, such as Liability or Professional Indemnity, can be claimed against," he says.

The WannaCry event has been more high-profile than other, more targeted and more damaging cyber attacks, he adds, and in that sense "might do some good if it increases awareness of this risk and the insurance that can be used to be protected against it".

Willis Towers Watson China's head of broker business, Wise Xu, says cyber risk will continue to creep up Chinese corporates' agendas: "The protection of IP systems in China is not that mature or sophisticated yet. So once [cyber attacks] become more targeted, it definitely will become a major issue."

"ANY INTRUSION THAT DISRUPTS SERVICES CAN LEAD TO BRAND AND REPUTATION DAMAGE, REGULATORY SCRUTINY, STAKEHOLDER DISSATISFACTION AND FINANCIAL LOSSES."

ABB (China) country insurance risk manager **Iris-Yan Ding**

InterContinental Hotels Group's Greater China head of risk management and insurance, Keith Xia, who is also a Parima China board member, agrees that the attack will focus corporates' minds on cyber risk.

ABB (China) country insurance risk manager Iris-Yan Ding says cyber risk is the biggest emerging risk on her radar in the next 12 months.

"Cyber security and information protection can be challenging for companies of all sizes," she explains.

"Hackers are not the only threat. Today's businesses rely on the internet for services such as online marketing, administrative functions, inventory management, credit card processing and distribution controls. Any intrusion that disrupts [the] delivery of these services can lead to brand and reputation damage, regulatory scrutiny, stakeholder dissatisfaction and financial losses."

Painfully clever criminals

What will the next generation of cyber threats look like? And how can these threats be mitigated by the insurance industry?

The volatile cyber risk landscape presents the insurance industry with an ever-changing threat. Hackers are sophisticated foes, always seeking new frontiers for their methods. So, what can we expect from the next generation of cyber threats, and can insurance help?

"What is so unique about cyber threats is that they are not bound by territory or a single philosophy," says Jason Kelly, AIG's head of liabilities and financial lines for Greater China, Australasia and South Korea.

"Who is targeted and how is always evolving and that can be influenced by monetary opportunity, a political agenda or ease of attack," he says.

While hacking a global bank and stealing sensitive information might come with a larger payout, he says, the amount of work and sophistication needed might divert hackers to easier targets.

Eamonn Cunningham, former chief risk officer at Scentre Group and Westfield, says the next generation of cyber threats will target those aspects of an enterprise's operations that are capable of inflicting the most pain. "The fundamental driver is, as always, commerce. How can I, as the hacker, extract most value for my time and effort?" he says.

"The ongoing developments in the robotics space and the advent of artificial intelligence are two areas where you can see great advantages for business and as a consequence, the likelihood of increased attention from hackers."

The insurance industry in turn will react to these new cyber threats, but AIG's Kelly says insurance should be considered the last line of defence when it comes to cyber and data security exposures: "No amount of insurance is enough if companies lack the required security controls, [while failing] to train staff or regularly update their software and controls.

"That being said, cyber exposures have been insurable in some form for nearly 20 years. Today, the insurance market has a lot of data points around first-party and third-party exposures, and insurance companies are constantly reviewing and updating their cyber offerings."

Kelly stresses that insurers, brokers, law firms and information technology companies constantly share information about legal liability, new regulations, new cyber threats, DDoS [distributed denial of service] attacks and settlements from data breaches.

Moreover, most of the main insurers have released a version of a standalone cyber insurance policy.

"There is a lot of information available from many parties," says Kelly, "and some insurers are also taking some of this global knowledge sharing in-house with cyber or data privacy experts in law, PR and IT."

"WHAT IS SO UNIQUE ABOUT CYBER THREATS IS THAT THEY ARE NOT BOUND BY TERRITORY OR A SINGLE PHILOSOPHY."

AIG head of liabilities and financial lines **Jason Kelly**

TRIAL AND ERROR

Cunningham, who purchased Scentre Group's first cyber insurance policy, says the insurance industry will invariably follow once the threats manifest themselves.

"Even then, the truly comprehensive market risk transfer response takes time to be developed," he says.

"There is an element of trial and error and unfortunately, there will be losses, large ones, before a fit-for-purpose product suite is available."

He says that like all stakeholders on the lawful side of the table, carriers and brokers will always be playing a rearguard action.

"Threats will constantly evolve – and since your starting point is always understanding exactly the type

45% of respondents cited risk assessment as their primary challenge in monitoring cyber risks

28% of companies that have suffered a cyber attack faced regulatory or law enforcement action and 26% lost customers

COMPANIES ARE STRUGGLING TO ADOPT A RISK-BASED APPROACH TO CYBER SECURITY

32% of organisations had conducted no risk assessment at all in the past year

of threats you face, the industry will continue to be in a reactive mode."

As for what risk managers need to know about the next generation of cyber threats, Kelly says the risk is continually evolving. Failure to understand and adjust for that will result in a data breach or malware intrusion, he says – followed by extortion and a public relations scramble, which ultimately damages the reputation of the company.

Cunningham stresses that risk managers do not need to become "cyber geeks".

"Leave that to more qualified and experienced people. Risk managers do, however, need to be aware that business is being impacted by a series of fast-moving, constantly evolving threats," he says.

"So, be very agile, as the associated risk velocity is constantly increasing. If you are lucky, the event may actually be on your doorstep before you even thought it existed. For others, it will have unknowingly come in your front door and out your back door."

He says risk managers must also rely on proven and trusted risk identification and assessment methodologies.

"Agility is particularly important when it comes to your response, so have the base response plan well rehearsed."

Risk managers must also obtain good-quality advise from experienced professionals, adds Cunningham, as living through one of the events brings more useful experience than simply talking about them.

53% of organisations evaluate their third parties' cyber security measures just by inserting a clause into their contracts to oblige them to adhere to security and privacy practices

35% of respondents said a third-party cyber breach had affected their organisation

34% of organisations stated that vetting third parties' cyber security standards is a challenge

THIRD-PARTY BREACHES ARE A GROWING CONCERN

SPONSORED WORD

UNDERSTANDING YOUR CYBER EXPOSURES

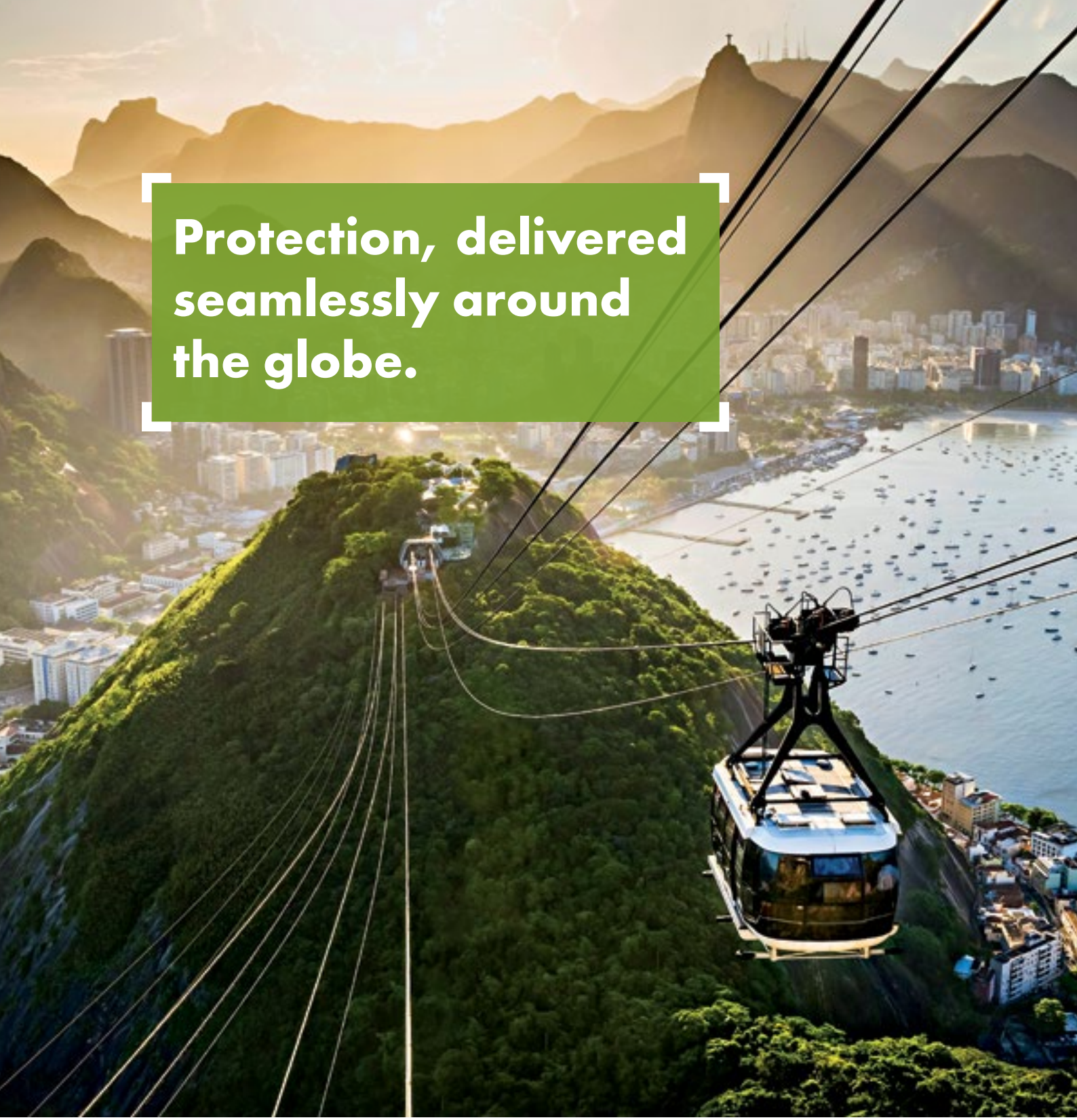
JASON KELLY
Head of liabilities and financial lines for Greater China, Australasia and South Korea, AIG

Cyber presents a dynamic risk landscape compared to that of traditional lines of commercial insurance. Within the many reasons attributed to this, the Internet of Things (IoT) and sharing economy both have a significant impact on the insurance industry. By 2020, spending on IoT will grow to $14.1 trillion, presenting a new set of risks concerning privacy and cyber security. This, in combination with the exponential growth of the sharing economy, which is projected to be a $335 billion market by 2025, means corporations face an ongoing challenge of safely acquiring, keeping and storing data.

We must therefore change the way we assess cyber risks in order to fully understand the extent of our clients' exposures. We do this through working hand-in-hand with the broker and clients' risk management team. Imperative to the assessment is collaborating with the clients' IT department, to identify the protections they have in place across the organisation, what type of data is acquired and retained, how many people have access to it, and what information, if any, is kept separate from the main network. Other fundamental factors also come into play, including the type of business, number of locations, and how revenue is collected. Moreover, the potential threat from the inside is often overlooked as there may be a lack of controls in place surrounding those that have access to sensitive data. Due to its complex nature, we are also seeing an increase in companies hiring external consultants to conduct a cyber-risk analysis as well as implementing recommended protocols.

Once a robust assessment has been completed, AIG works with the broker and client to pinpoint the most crucial risks and review the exposures the client is most concerned about. From there we will recommend mitigation procedures and provide the best insurance solution with the right protection.

› For more, visit www.aig.com/hk



Navigating a complex world can be challenging.

Wherever your business takes you, AIG is there to help you manage your risks with confidence. Together, we take a proactive approach to build the optimal multinational program to meet the needs you have today, and support the goals you have for the future. Refined over nearly a century—we put our insights, expertise, and world class service to work for you. Learn more at www.AIG.com/multinational

AIG®

Bring on tomorrow