NOVEMBER 2017

CASUALTY MATTERS®


# Cyber Insurance Ready for Take-Off in China

*by Frank Wang, Gen Re, Shanghai*

The WannaCry ransomware worm that hit organisations in 150 countries around the world took awareness of cyber risk to a new level in 2017. In China, where computers at nearly 30,000 institutions were infected by the deadly virus, the attack served as a loud wake-up call.

Cyber risk was already a hot topic in China after the implementation in June 2017 of data privacy rules that place new obligations on businesses. This law, along with the growing frequency of malware attacks, is leading more businesses in China to look for cyber risk transfer solutions.

Not surprisingly, insurers are responding to this growing awareness of cyber risk, developing innovative insurance products and services that will help businesses protect themselves against the costs relating to complex first-party expenses and third-party liabilities.

However, despite the vast cyber insurance market potential that exists in China, numerous challenges still need to be addressed before it can be realised.

The Cybersecurity Law of the People's Republic of China (PRC) promises to make businesses think harder about the different liabilities they will face when hit by malware or a data breach.

The new law contains six important clarifications, namely:

- The principle of cyberspace sovereignty
- The security obligations of network product and service providers;
- The security obligations of network operators
- Personal information protection rules
- A system for protecting the security of critical information infrastructure (CII)
- Rules for cross-border transmission of important data related to CII

## Content



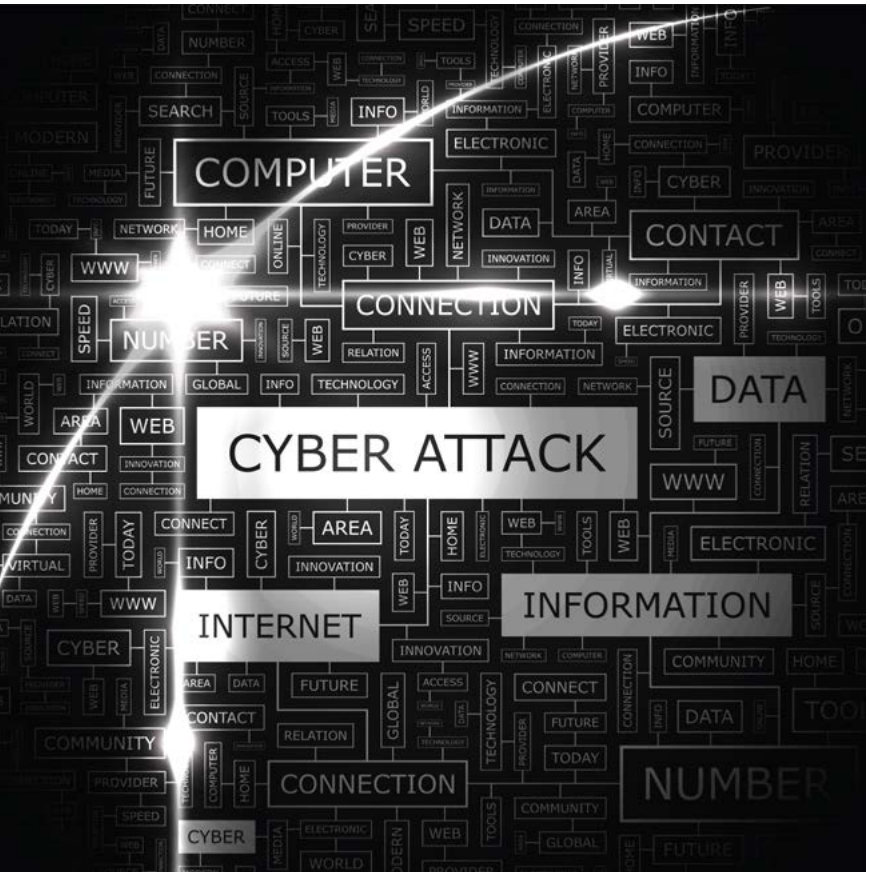
## About This Newsletter

*Casualty Matters* reviews new liability developments affecting General Liability, Commercial Umbrella and Personal Umbrella business. Our underwriters provide perspectives on the developments mean to insurers and specific types of insureds.

Among those clarifications, with respect to personal information leaks, the new cybersecurity law includes the following stipulations:

- Network products and services must be able to collect user information, and their providers should state this explicitly to users and obtain their consent.
- Network operators shall not reveal, tamper with or damage the personal information that they have collected.
- No individual or organization may steal or obtain personal information by some other illegal means and may not illegally sell or provide personal information to others.

However, the most important clause of the new cybersecurity law in relation to cyber insurance is Article 42. This article stipulates that "network operators shall adopt technical measures and the other necessary measures to ensure the security of the personal information that they have collected and prevent the information from being leaked, damaged, or lost…[U]nder circumstances in which the leakage, damage, or loss of personal information has occurred or might occur, they shall immediately adopt remedial measures and notify users in a timely manner in accordance with the provisions and report to the relevant department in charge."




The provision makes clear the statutory notification and remedial obligations of network operators, including the owners and administrators of networks and network service providers, when a leakage of personal information occurs.

In addition, the law also stipulates: "In the case of an act that breaches the Cybersecurity Law, the personnel and companies that are directly responsible must bear their civil liabilities in addition to bearing their administrative and criminal liabilities."

The new law clearly establishes a solid legal foundation for the development of cyber insurance in China, as has already happened in other countries. Such a precedent was set in the U.S., where the fast evolution of the cyber insurance market is widely attributed to the introduction of the Data Security and Breach Notification Act in every state during the past decade.

## China and the Global Cyber Insurance Market

In China, people's anxiety about network risks increases with each passing day. A cybersecurity research report from Allianz Insurance indicates that China suffers USD60 billion economic losses annually due to cyber attacks.[1] It puts China at the top of the loss league table in Asia and second to the U.S. in the world ranking.

In terms of distribution of the global cyber insurance market, North America is the largest market for cyber insurance, accounting for 90% of the total. Although the cyber insurance market in Europe is less developed compared with the U.S., it too is poised for rapid development. The General Data Protection Regulation (GDPR) directive, which compulsorily requires companies to issue notice of security breaches, comes into effect in May 2018 and is expected to trigger strong demand for cyber insurance across Europe.

In Asia, cyber insurance penetration is still low but demand is increasing, with insurance products spreading gradually from Europe and the U.S. to emerging markets such as China. As mentioned, the implementation of China's Cybersecurity Law

in June 2017 – as well as numerous cybersecurity incidents – will prompt more businesses in China to explore insurance protection.

Comprehensive cyber insurance is already available in China from foreign-invested insurance companies. The coverage available is divided into three parts and covers first-party economic losses and third-party legal compensation liability, as described in the following cases and relevant coverage:

- Economic losses that are incurred due to the disruption of normal operations caused by hacker attacks – compensation of businesses for some of their costs, excluding normal operating expenditures, during the time when system security is ineffective
- Costs that are incurred when a company hires an authentication services advisor to verify whether or not a data security accident has already occurred – provide recommendations on how to avoid or reduce data security accidents
- Legal costs and expenses that are incurred in data breach disclosure to the information owners – can also include reimbursing expenses that are incurred when hiring independent professional public relations consultants to reduce damage to its reputation

## Challenges and Countermeasures

In the third quarter of 2016, Pricewaterhouse-Coopers' forecast, "Insurance 2020 and Beyond: Reaping the Dividends of Cyber Resilience", said that the global cyber insurance market will increase to USD5 billion by 2018 and USD7.5 billion by 2020.

An April 2017 report from the U.S. Council of Insurance Agents & Brokers (CIAB) showed that in the U.S., where the cyber insurance market is relatively mature, about 32% of commercial institutions have purchased cyber insurance; the average limit of liability purchased grew to USD6 million compared with USD3 million in October 2016.

In comparison with North America and Europe, the cyber insurance market in China is at an early stage of development.

### Cyber Attacks: A Growing Global Threat

In May 2017, a form of ransomware called "WannaCry" started to infect computers around the world, encrypting computer information and demanding money for the decryption.

According to reports, businesses in more than 150 countries fell prey to the WannaCry ransomware. Dozens of hospitals in the UK were forced to suspend emergency and other services, hundreds of computers of the Russian Federation Ministry of Internal Affairs were attacked, as was the German railway system and the U.S. logistics company FedEx.

In China the computers at nearly 30,000 institutions were infected by the deadly virus.

It has been reported that the "WannaCry" ransomware caused USD8 billion in direct economic losses around the world. As many affected companies had not bought cyber insurance, they had to bear the substantial financial losses themselves.

The WannaCry attack was followed in June by a similar fast spreading virus called Petya, which also hit big brand-name corporations around the world, including Nurofen-maker Reckitt Benckiser, Oreo cookie manufacturer Mondelez International, the shipping group Maersk and the advertising agency WPP.

From an insurer's perspective, three main issues slow the development of cyber insurance in China:

- The lack of a more sophisticated legal and regulatory support system
- The absence of historical loss data for effective underwriting and product pricing
- Inadequate cybersecurity risk management resources

While the basic rules for protecting personal information have been established with the Cybersecurity Law of the PRC, as mentioned earlier, the relevant supporting details for implementation are still not perfect. Furthermore, in terms of the serious reality of misuse of personal information in China, the number of legal provisions for data protection remains relatively limited. The scope of application is relatively narrow and there is no uniform personal data protection law that applies exclusively to all information controllers.

At the same time, data protection rules apply more to "criminal punishment" and "administrative management" than the determination of "civil liability". As a result, even though a business can be subject to punishment after a data breach, it may not be possible to obtain any substantive civil damages.

In connection with these problems, the state is currently promoting the legislative process of a Personal Information Protection Law. At the same time, the Cyberspace Administration of China has issued a series of detailed rules for implementing the Cybersecurity Law.

In order to set up a sophisticated legal basis for cyber insurance, the relevant laws and regulations must ease the judicial process, not only stipulating the confidentiality obligation for personal information but also making clear the legal consequences of violating the said obligation, in particular the standards for civil damage compensation.

## Underwriting Cyber Risk

Understanding how to underwrite and price cyber risk has been a challenge in all markets. Standalone cyber insurance is an entirely new kind of insurance; the history of its development is very short and we have no experience of another sophisticated market from which to learn. In addition, cyber risks change from one day to the next.

Cyber insurance has been available in China for only a few years and, again, practically no loss experience exists that can be used as a reference. Moreover, the channels through which insurers can obtain basic information for effective pricing are extremely limited.

The number of cybersecurity incidents that are publicly reported in China is far smaller than the number that has actually occurred, making it difficult to express the actual cyber risk level in China with the public historical loss data that is available. As a result, insurers are advised to adopt a prudent underwriting policy and "cross the river by feeling the stones": in other words, develop the business while accumulating the lessons of experience at the same time and then make adjustments and corrections in a timely manner.

Cyber security risk management is another technical challenge and it requires the participation of cybersecurity professionals throughout the entire process. This is crucial for insurers because pre-underwriting risk assessment, post-underwriting risk control, and loss adjustment after losses are incurred all require cooperation with cybersecurity experts.

In the U.S., almost every cyber underwriter and broker that is developing a cyber insurance business has partnered with at least one cybersecurity advisory company. In recent years, a number of cybersecurity science and technology start-ups for insurer services have appeared as a result of the rapid development of cyber insurance in the U.S.

Although China already has many companies engaged in work related to cybersecurity, it still lacks companies that can provide modelling and pricing support to insurers. However, in line with the gradual rise in cyber insurance demand in China, some cybersecurity companies that were originally not involved with the insurance business are currently investigating cooperation with insurance companies.

Their aim is to jointly develop comprehensive solutions for cyber risks, including risk assessment, monitoring and early warnings, emergency response and insurance coverage.

In conclusion, although there are still challenges ahead, the roots of a sustainable cyber insurance market seem to be taking hold in China.

### Endnotes

1 http://www.agcs.allianz.com/insights/white-papers-and-case-studies/cyber-risk-guide/.
2 https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.

## About the Author

**Frank Wang,** CPCU, RPLU, ARe, is the Liability Specialist and a Senior Treaty Underwriter in Gen Re's Treaty department in Shanghai. He is responsible for developing and underwriting liability treaty portfolios and acts as the key advisor on liability insurance/reinsurance and other liability-related industry issues.

He can be reached at +86 21 6100 6318 or frank.wang@genre.com

For more articles on "China Liability Insurance", please click here:
genre.com/casualtymatterschina

Or scan the following QR code directly.

Read our Cyber articles and blogs in English at
genre.com/cyber

**General Reinsurance AG**
Shanghai Branch
Room 1803, China Merchants Tower
161 East Lujiazui Road
Shanghai 200120
Tel. +86 21 6100 6300
Fax +86 21 6100 6388

*Photos: © Thinkstock: istock, Kirill_Savenko, zjzpp163, StudioM1*

*The difference is...the quality of the promise®*

genre.com | genre.com/perspective | LinkedIn: linkedin.com/company/gen-re