Brace yourselves: Global cyberinsurance demand is coming

By Dan Twersky, Andrew Ko, and Judy Xiang

While cyber liability insurance is one of – if not *the* – fastest growing type of products in the industry, the majority of that growth has historically come from U.S. purchasers.

The U.S. – where the regulation resides

The most plausible explanation for the rapid rise of cyber liability insurance in the U.S. – and not elsewhere – is that individual states (well, at least 48 of them) and the federal government have been at the forefront of privacy legislation by enacting strict data breach notification statutes.

The effect of this legislation is multi-faceted, but naturally involves business cost. First, because many of these laws follow the states of residence of the affected individuals as opposed to the location of the breach or the breached entity, an incident affecting a large enough population will likely require an analysis of each of these laws, many of which have different definitions as to what exactly constitutes a breach requiring notification, and varying requirements as to the method, timeliness, and wording of the notification. Second, to the extent legal counsel determines that notification is indeed required, the organization will incur the cost of transmitting the notice (usually by regular mail), and often, depending on the type of information compromised, the notice will include credit/identity theft monitoring and fraud resolution services. Finally, to the extent any regulators take an interest in the incident, there is a risk of a fine or penalty being assessed. Recent examples include an $18.5 million settlement between a retailer and 47 states and the District of Columbia, and a $5.55 million settlement between a health system and the Department of Health & Human Services Office for Civil Rights.

The new frontier

Outside the U.S., and without the regulation-driven costs, there has understandably been less of an interest and/or perceived need for cyber liability insurance. But that lack of demand appears to be dissipating rapidly. What's changed?

For starters, there has been an evolution in both the manner and purpose of cyber attacks, most notably ransomware. According to security firm SonicWall's 2017 Annual Threat Report, ransomware use grew 167 times year over year, as the 3.8 million attack attempts in 2015 rose to 638 million in 2016. Hackers have concluded that instead of spending a great deal of time attempting to infiltrate a targeted organization's network through a backdoor security hole, it's easier to trick one of the organization's employees into opening the front door. What's more, according to Symantec's 2017 Internet Security Threat Report, the average ransomware extortion demand rose to $1,077 in 2016, up from $294 in 2015, and those numbers are expected to rise as attackers shift their focus from individual consumers to businesses.

Whereas the goal used to be to make a quick hit, recent ransomware incident reports indicate that attackers are conducting significant research on their victims. In June, a cloud services provider had 150 of its servers encrypted, resulting in outages to the sites of more than 3,400 of its business customers. The ransom demand was purportedly negotiated down from an initial demand of over $4 million to approximately $1 million (a record amount — *for now* — in terms of publicly reported ransomware payments). What is so noteworthy about this particular demand is not so much the amount, but the way in which it was derived; it has been reported that the hackers based their demand on a calculation of the cloud provider's total annual payroll. Accordingly, it seems that attackers in the future are more likely to make demands that take into account the financial means of their victims. It remains to be seen just how high that number can go before an affected organization decides it's not worth recovering the encrypted data.

While the increase in ransom demand amounts may finally be tempting non-U.S. organizations to purchase cyber liability insurance, it's more likely that the consequences of *not* paying the ransom has them apprehensive. To the extent that: a) the affected organization refuses to pay the ransom; b) the hacker does not live up to their end of the bargain and fails to provide the decryption key; or c) the decryption process fully or partially fails and causes corruption of the data at issue, the effect could very well be an extended period of business interruption. The inability to earn income due to a network disruption is something to which any modern day organization can relate. Recent mass scale *WannaCry* and *Not-Petya* ransomware attacks have caused business interruptions of varying degrees to companies of all sizes. It is this system outage coverage that has served to convince many insurance buyers — even those with little to no risk of regulation-driven cost exposure — that there is still relevant and valuable protection available within a cyber liability insurance policy. Moreover, the number of organizations around the world with little regulatory exposure is decreasing.

Privacy regulation outside the U.S.

We previously provided a comprehensive look into the EU's GDPR, which is set to apply from May 25, 2018 following a two-year transition period. What has not received as much attention is China's 79-article Cyber Security Law ("CSL"), which took effect on June 1, 2017, and is likely to impact companies with a presence in China and those doing

Whereas the goal used to be to make a quick hit, recent ransomware incident reports indicate that attackers are conducting significant research on their victims.

business with China. As a basic law, the CSL is an important starting point for personal information protection and regulation of cybersecurity risks. It is expected that a series of rules and regulations will be released to work alongside the CSL. However, in the meantime, many businesses potentially affected by the CSL have criticized the law as being vague, and overly broad in scope.

The CSL applies to the construction, operation, maintenance and usage of networks, as well as the supervision and management of networks within the mainland territory of China. A heavy focus is placed on "network operators," defined by the CSL as owners and administrators of networks. Because that definition is incredibly broad, organizations that provide services and conduct business activities through networks may unknowingly be considered network operators. In addition to traditional telecom operators and internet firms, the definition of network operators could possibly be construed to include banking institutions, insurance companies, IT security companies, and other enterprises that have websites and provide various network services.

Network operators must adopt measures to safeguard network security and stability, respond to network security incidents, prevent cybercrimes and unlawful activity, and protect online data. In addition, certain network operators providing critical information infrastructure services or support have more stringent requirements, including training employees, formulating emergency response plans, and conducting disaster recovery exercises.

Perhaps the most significant impact of the CSL from an operational and financial standpoint will be on foreign and multinational organizations. The CSL stipulates that critical information collected or generated in China must be stored domestically. The only way to transfer that information outside of China is to allow security assessments to be conducted by Chinese regulators.

For individuals, the protections around personal information are strong. Network operators are barred from disclosing, tampering with, or destroying the personal information they have collected, while individuals and organizations are forbidden from stealing or using other illegal means to obtain personal information.

Companies that violate the CSL risk the suspension of operations, cancellation of business permits, imprisonment, and the assessment of monetary penalties of up to 10 times the amount of unlawful gains (or up to 1 million Renminbi — approximately $150,000 USD).

Despite the concerns about the CSL being vague and/or overly broad in its scope and application, those organizations conducting business in and with China should thoroughly review the CSL in connection with their current policies and procedures governing network security and data privacy.

Going global

These developments in China illustrate that what has largely been a U.S. market for cyberinsurance so far may not remain that way for long. The ever-present risk of business interruption resulting from cyber attacks, such as ransomware, the global increase in data security and privacy regulation, and the potential fines and penalties exposure associated with non-compliance, are steadily fueling international demand for cyber liability insurance. When implemented as a risk protection solution along with assessment and recovery planning tools, cyberinsurance provides organizations with a holistically sound approach to cyber risk management.

Contact

Dan Twersky
212.915.8580
Dan.Twersky@willistowerswatson.com

Andrew Ko
+ 86 21 5029 8021
Andrew.Ko@willistowerswatson.com

Judy Xiang
+86 21 5029 8063
Judy.Xiang@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW-GL-17-PUB-8053a1c

willistowerswatson.com

Willis Towers Watson