Advisen
Transforming • Insurance™

THE GLOBALIZATION OF THE CYBER INSURANCE MARKET

Sponsored by

CYBERSCOUT™

May 2017

INTRODUCTION: INSURANCE FOLLOWS REGULATION, LITIGATION

In the world of cyber insurance, there are leaders and laggards, but research suggests that although the United States leads, by far, in cyber insurance take-up rates, many other parts of the world are warming up to this risk-transfer and mitigation strategy.

Driving this shift are regulatory and legislative initiatives in a number of regions, as governments attempt to standardize cyber security protocols and notification requirements and set consequences for organizations deemed to not be in compliance. Cyber security regulations are undergoing seismic changes in substance and scope across the globe.

Litigation also can play a role in an organization's appetite for a cyber insurance product. Especially—if not, for now, exclusively—in the United States, legal expenses following an event are one of the main drivers to shore up network security and purchase cyber insurance. But this, too, may be changing as other parts of the world look to the courts to settle disputes related to privacy and network disruptions.

However, according to CFC Underwriting cyber product leader James Burns, "Legislation and regulation move at different speeds in different countries."

This paper will examine the following, by region:

- An overview of the cyber insurance marketplace
- Reasons businesses are buying cyber insurance
- Challenges and opportunities ahead

No organization, regardless of size, industry or location, is immune to cyber incidents. Breaches, cyber attacks and privacy violations are commonplace, and reports indicate the techniques used today by hackers seeking valuable personal and financial information will continue to haunt businesses for years to come. This does not mention insider threats, which also can cause significant business consequences.

Every organization needs cyber insurance to manage its exposures, but the take-up rates differ by region as organizations begin to find the value in this risk management solution.

"Most organizations are aware of the risk by now, and most are making plans to maintain a strong information security posture," said Andy Obuchowski, Charles River Associates' vice president. "Insurance, and the services that come with most policies, should be a part of the plan, and more and more companies around the world are realizing this."

UNITED STATES: LEADER IN CYBER INSURANCE TAKE-UP

No place is the purchase of cyber insurance more commonplace than in the United States. It is estimated that U.S. companies account for about 90 percent of all cyber insurance purchases. The take-up rate typically can be agreed to be between 25 percent and 30 percent, which is much higher than in other regions of the world. Cyber-related risk—whether data breach, fraud, theft or network disruption—often is cited by U.S. executives as one of the top risks their businesses face.

The regulatory and litigious environment in the United States motivates the purchase of cyber insurance. Regulatory and legal factors have led to a more rapid awareness of the need to invest in a mature cyber security posture, which includes insurance protection. Litigation in the United States, as well as fines and penalties from regulatory

authorities, bring the issue to the forefront much more so than in other regions because both add potentially financially damaging impact to a cyber incident, which often is fodder for news headlines.

“Most of the business is happening in the U.S. because there are a number of regulations and a focus on security and privacy with organizations,” said Burns of CFC Underwriting.

Privacy exposures from data breaches were first recognized in highly regulated industries, such as healthcare, retail and financial institutions. A cyber attack against a company in these industries can lead to state and federal scrutiny pertaining to notification requirements, and often has been followed by litigation from consumers, investors, authorities or payment providers. This has been a primary driver of the use of cyber insurance as a clear risk-transfer method, said Ryan Griffin, a senior vice president of JLT Specialty USA’s Cyber/E&O Practice.

Other industry classes, such as energy and manufacturing, have since recognized the value of cyber insurance and services as they “see the potential of cyber-related incidents causing disruptions to business operations,” Griffin said.

“Cyber risk extends beyond that of the exposure related to personal and financial information, such as theft of proprietary information,” Obuchowski said. “This is an operational risk for all businesses of all sizes.”

There are, however, some challenges in the U.S. cyber insurance marketplace. Although the take-up of cyber insurance products among small and midsize companies has increased in recent years, they have yet to purchase coverage at a rate anywhere near their large-company peers. This may be due to several factors including lack of exposure knowledge, awareness of the product’s value and services, and the expenditure involved.

The competition among insurers for middle-market business is hot. After all, there are many more businesses in this revenue category than there are large businesses, and a relative drop in some large-loss claims from the bigger corporations has resulted in more insurance capacity.

UNITED KINGDOM, EUROPE, CANADA AND AUSTRALIA: PLAYING CATCH-UP, INCREASING THE PACE

JLT’s Griffin said other regions of the world are “catching on” to cyber insurance as a solution.

According to Tom Spier, director of business development for the U.K. and international markets at CyberScout, cyber crime and ransomware currently are the primary drivers of companies looking to buy cyber insurance in these markets. For instance, he called Australia the “identity theft capital of the world.”

“It’s all about emphasis,” said Burns of CFC. “You don’t have the same types of environments as you see in the U.S., so there is less focus on privacy right now. The discussion focuses primarily on first-party exposure and business interruption centered on cyber crime, social engineering and phishing [in the U.K.].”

Burns said the same could be said for Australia, which “looks more like the U.K. than the U.S.”

Spier said companies in these regions are “looking to fill gaps that their traditional insurance policies do not cover or specifically exclude.” He said the costs related to data breaches also are being realized, garnering additional attention toward risk-transfer solutions.

The litigious culture of the United States does not exist in other countries or regions, but that could change somewhat as the legislative and subsequent regulatory environments in these regions put pressure on businesses when it comes to cyber risk—especially when it comes to privacy.

Burns said Australia and Canada are each mulling initiating or updating privacy legislation related to cyber risk that could "up the ante" and "open up some different angles" in the case for cyber insurance. It also could open up some avenues in the courts as a matter of recourse. Spier said Australia's new mandatory notification laws could result in some class-action litigation. "Litigation is quite common," he said of Australia.

However, Australia is a "relatively small market," said Spier, with available insurance limits high, relative to premiums. So, it is more difficult for insurers to make money.

In Europe, much of the talk has to do with the European Union's General Data Protection Regulation (GDPR), which is meant to harmonize data privacy laws across Europe. It also outlines strict penalties against companies that do not comply—up to 4 percent of global revenues.

Griffin said the GDPR is "arguably more onerous" than privacy laws in the United States. "The fines associated with the regulation are punishing," he said, adding that companies are buying insurance now in advance of GDPR enforcement, set for May 2018.

There is a lot of uncertainty whether GDPR will be enforced in the U.K. following its exit from the European Union, but many companies are working under the premise that even if the GDPR is not in play, a similar directive will be in place.

It shouldn't go without saying that companies anywhere who ignore GDPR "do so at their own peril," Spier said. All companies, no matter where they are based, that offer goods and services to EU citizens are just as exposed to the regulations.

FINDING OPPORTUNITIES IN REST OF THE WORLD

Cyber insurance in the rest of the world is similarly affected by a region's regulations on companies, which could be specific to an industry. Financial institutions in many regions are heavily regulated, and reports indicate banks in various countries are turning to cyber insurance protection to avoid regulatory scrutiny or punishment. As a result, banks then put pressure on service providers by requiring them to demonstrate robust cyber security in order to get business.

However, the sale of cyber insurance in many regions also is influenced by cultural factors.

For instance, there may be language barriers or obstacles having to do with Islamic law in the Middle East. Many large companies in Asia, Spier explained, are family-owned, and they may not be willing to share cyber security information—preferring instead to keep risk in-house. Japan has different views of insurance as a strategy.

Additionally, underwriting may not be as easy as in some other regions because cyber security maturity and readiness are low. According to reports, cyber security is just becoming a priority for many companies.

Infrastructure can be limited in many parts of the world, where business can be conducted primarily on out–of-date and/or pirated operating systems, or even hand-held devices. Or, laws and regulations in a certain country also may make it difficult to launch a product.

There are exceptions, and potential opportunities for insurers to explore, in some significantly developed parts of the world, such as Dubai in the United Arab Emirates. Brokers also mentioned China, Israel, India and Brazil as potential growth areas, but there is a "precipitous drop-off after that," Griffin said.

EDUCATE AND NURTURE

Selling cyber insurance in any of these markets often is a matter of education to pitch cyber insurance as a necessary risk-management strategy for any company, just as they would buy property insurance. Even in the United States, there are pockets of potential buyers—mainly in the middle market—where this is true.

But in order to make the case, in the face of a lack of regulation in many places, Burns said cyber insurance needs to be marketed differently.

“The pitch so far has mostly been about privacy, but when you try to transport that elsewhere, it doesn’t make sense for them because they may not have the same privacy exposure,” Burns said. “All businesses face cyber as a business continuity risk.”

After all, cyber insurance products are more than risk-transfer. Many policies are services contracts, with extensive pre- and post-event packages to mitigate losses with the help of cyber security vendors and attorneys.

Australia is a good case in point, Burns said. The island continent was overlooked and underserved, but once potential buyers were educated and nurtured, insurance began to look like a better idea to assure business continuity.

“Companies will need to know that cyber insurance responds in the right way and is applicable to 40 different countries, in multiple languages,” Spier said. “Once buyers see that, I think the value of this product will become immediately obvious. ”

Some analysts predict the cyber insurance market will grow to $20 billion in premiums by 2020, but it is not on pace to do so. Spier said insurers need to “wake up” and “respond to exact situations in each country around the world.”

“You need the local knowledge to find out what they fear the most when it comes to this risk,” Spier said.

The insurance community is making efforts to inform new regions of cyber risk, and they are hoping the investment translates to insurance purchases.

“We’ve done a ton of education for clients. It takes a long time for the message to make its way around the globe,” Griffin said. “They are all aware of the risk, but they may think they can quantify it—that it doesn’t merit insurance. “

Obuchowski said companies can’t have that attitude. “You can’t buy security off the self, and thinking you have [cyber risk] under control could be more dangerous,” Obuchowski said. “Having a device is one step closer—it’s a tool. Insurance needs to be another one of those tools in the risk-mitigation toolbox.”

Unfortunately, it may take a global cyber event—or large, localized events—for companies to realize the need for cyber insurance.