Carrier Management

Buyers Aren't Happy With Their Cyber Insurance: J.D. Power

Written by David Pieffer | Published February 28, 2018 on CarrierManagement.com

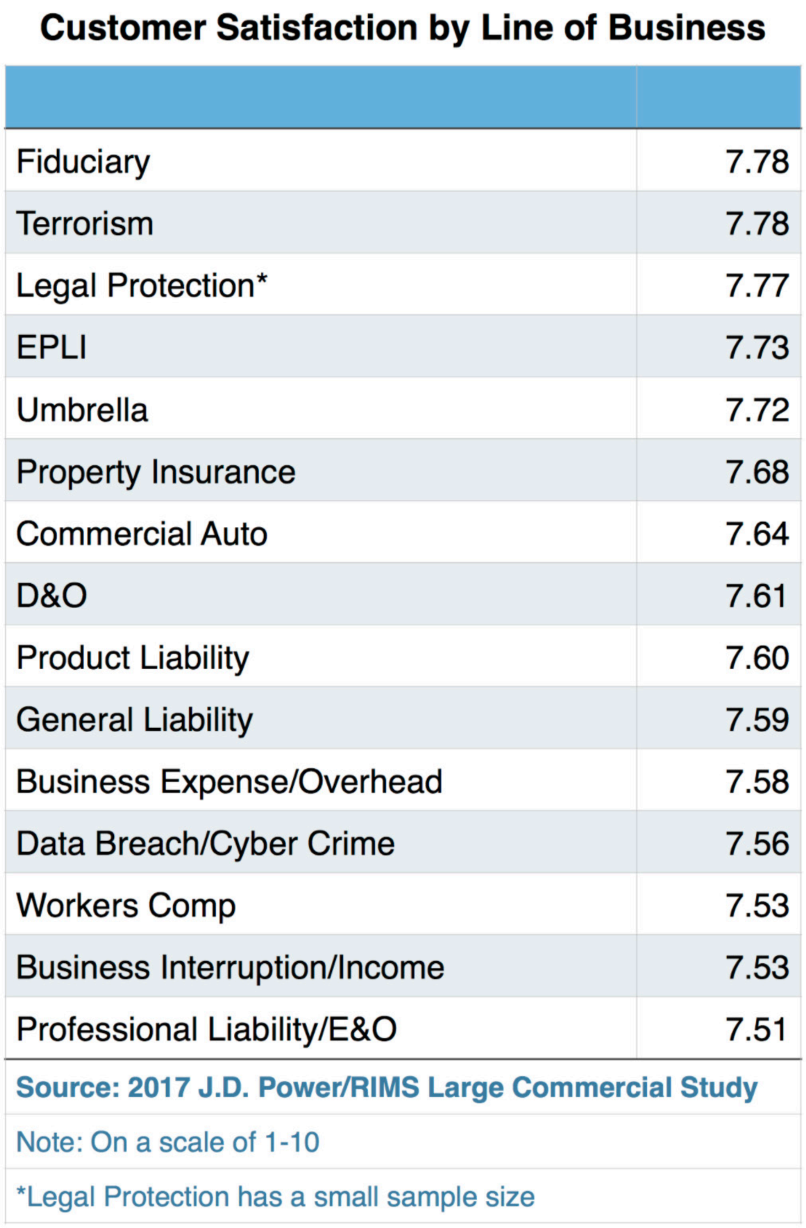
On any given day, it is hard not to read an article or report on some type of cyber topic. Cyber insurance is one of the key concerns within the insurance industry today and possibly one of the most misunderstood.

In late 2017, Advisen in partnership with Partner Re reported that 62 percent of the agents and brokers they surveyed felt cyber coverage was becoming more consistent but that it still was hard to compare policies between carriers. The report also noted that the industry was split on whether cyber property damage should be covered by the property policy (44 percent) or the cyber policy (40 percent). The takeaway: Agents not understanding the exposures and coverages is the main obstacle to selling cyber insurance. (Advisen-Partner Re: 2017 Survey of Cyber Insurance Market Trends) Further exacerbating the situation is the fact that cyber liability, business interruption and property coverage all potentially apply, in some degree, to cyber-related claims. Knowledge of the cyber-related particulars of these coverages is particularly important when determining which policy is triggered depending on how the incident occurred and relative to the other policies.

Clearly, this developing area of risk is one that can be confusing for insurance professionals and even more so for insureds. In the 2017 J.D. Power/RIMS Large Commercial Study, the survey of more than 1,200 risk professionals found that the respondents were least satisfied with the industry's response to cyber insurance. There was a lack of confidence in the handling of cyber products, including liability, physical damage, business income and business interruption. As one respondent said:

"I think more emphasis on assisting with the preventive aspects of cyber losses—loss control, training, pre-loss resourcing of business partners who will respond postloss—would attract a bigger response. There are so many hidden and unknown sides to this exposure that clients require more education and hand-holding to perceive their insurers as partners."

As found in the survey, customers have a low level of satisfaction related to cyber products, generally viewing them as a specialty line and expecting carriers to have the expertise and capability to handle this line of business. So far, there is a lack of customer trust in the industry's ability to deal with this exposure. There also are strong feelings that both claims and loss control lack the capabilities to handle the exposure or to provide the kind of risk management support customers need to address their financial, reputational and operational exposures.



Customer Satisfaction by Line of Business

Fiduciary	7.78
Terrorism	7.78
Legal Protection*	7.77
EPLI	7.73
Umbrella	7.72
Property Insurance	7.68
Commercial Auto	7.64
D&O	7.61
Product Liability	7.60
General Liability	7.59
Business Expense/Overhead	7.58
Data Breach/Cyber Crime	7.56
Workers Comp	7.53
Business Interruption/Income	7.53
Professional Liability/E&O	7.51

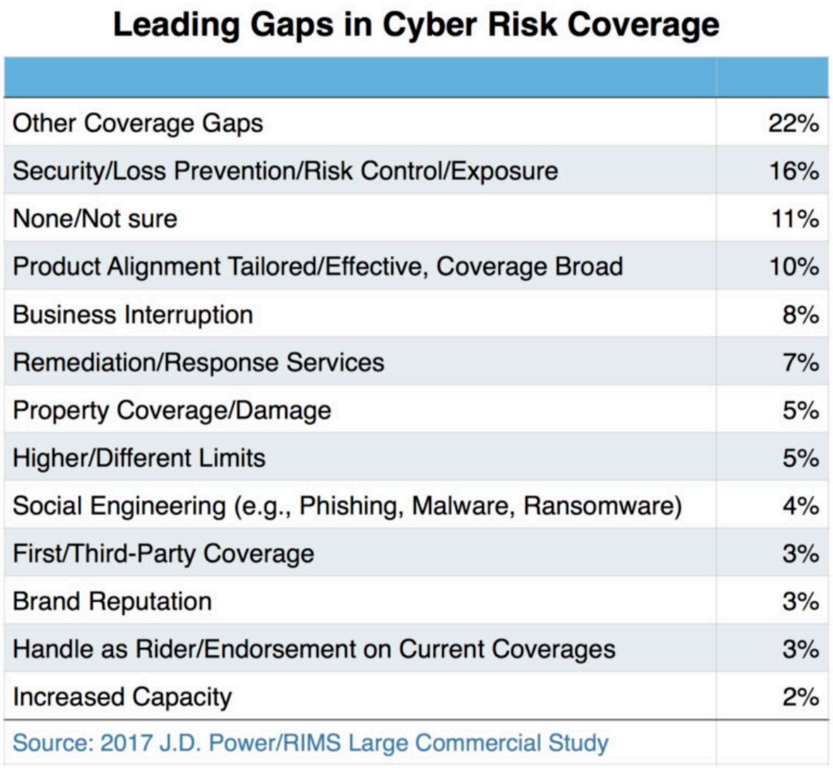
Source: 2017 J.D. Power/RIMS Large Commercial Study

Note: On a scale of 1-10

*Legal Protection has a small sample size

The low satisfaction scores for cyber products are fueled by a lack of understanding by the customer of the coverage being provided compared to what the customer believes they need. The survey also found that one-third of the respondents either didn't know or thought there where additional coverage gaps in their cyber program. Given the respondents to this survey were all insurance/risk professionals, the lack of clarity related to cyber coverages points to the monumental task the industry faces to provide more information and insight about their policies.

Respondents also identified gaps in risk and loss prevention (16 percent) and product alignment (10 percent), suggesting carriers need to provide more communication and clarity related to loss prevention and risk structuring services. Carriers must be able to better educate customers and brokers about the alignment of potential risks and the coverages, risk mitigation and claim management services that are needed related to cyber specific risk.



Leading Gaps in Cyber Risk Coverage

Other Coverage Gaps	22%
Security/Loss Prevention/Risk Control/Exposure	16%
None/Not sure	11%
Product Alignment Tailored/Effective, Coverage Broad	10%
Business Interruption	8%
Remediation/Response Services	7%
Property Coverage/Damage	5%
Higher/Different Limits	5%
Social Engineering (e.g., Phishing, Malware, Ransomware)	4%
First/Third-Party Coverage	3%
Brand Reputation	3%
Handle as Rider/Endorsement on Current Coverages	3%
Increased Capacity	2%

Source: 2017 J.D. Power/RIMS Large Commercial Study

The Large Commercial Study also found that as customers try to understand whether they currently have the right coverage, they also are undecided about what their future needs might be related to cyber insurance. Respondents predominantly cited “other drivers” (29 percent) as the future drivers of cyber risk. This underscores the challenges insurers have in understanding the nature of cyber risk and how it complicates their ability to navigate the choice of insurance tools to address it. Such uncertainty belies the need insureds have for quality advice, service and education related to cyber risk and what drives it. Among respondents there is little consensus on what is driving or will drive cyber risk going forward, but those most commonly mentioned were:

- **Social engineering (e.g., phishing, malware, ransomware)**—14 percent: Attacks have been growing in frequency and severity and are often crippling and destructive to organizations.
- **Advancements in technology/Internet of Things (IoT)**—13 percent: As companies become more reliant on technology and systems become more integrated and connected, comments indicate this will lead to greater exposure and vulnerabilities to a host of devices and networks.
- **Insurance product alignment, customization and breadth**—10 percent: Comments underscore the need for alignment of insurance products, standard languages and broader coverages.
- **Breaches leading to data corruption or theft (intellectual property, identity)**—8 percent: General breaches and breaches leading to data corruption or theft of intellectual property and identities also are leading concerns.

Findings of the Large Commercial Study reported a strong alignment between current coverage gaps and future drivers related to cyber risk. This alignment shows there is both an immediate and ongoing need for greater loss prevention services, risk mitigation strategies, insurance product alignment, clarity of coverage, and greater coverage options. Carriers must rethink how they develop their products and staff, how they educate agents and brokers, and how they market and sell cyber policies to their customer base. Even though the study discussed here was focused on large commercial carriers, the issues are not limited to large companies such as Merck or Toyota. The problems are equally as important for middle-market companies and small businesses.

Smaller firms are much less likely to have the ability or time to put in place elaborate or extensive security precautions, yet their exposures are just as real. Even individuals are not immune to a cyber event given the growth of individual-focused technologies like autonomous (self-driving) cars, drones, smart vehicles, smart homes and the 62 percent of adults in the United States using online banking. (Creditcard.com; Online and mobile banking statistics, Jamie Gonzalez-Garcia, March 20, 2017) Clearly, there is or soon will be a need for robust cyber insurance products in the personal lines market also.

According to PricewaterhouseCoopers (PricewaterhouseCoopers, Insurance 2020 & beyond: Reaping the dividends of cyber resilience), the U.S. cyber market is the fastest-growing line in the insurance industry and will grow nearly 300 percent over the next two years to $7.5 billion. With so much uncertainty in the market, carriers can't simply put out a piecemeal cyber strategy. The strategy must be clearly defined and aligned with the other standard lines of business (property, liability, inland marine and BI, among others) to answer customer needs and concerns. This should include strong loss prevention and risk mitigation plans, knowledgeable claim organizations, and effective educational processes for customers and agents/brokers. Carriers must build and manage cyber products with the understanding that the cyber coverages will become fully integrated with property, liability and personal auto/homeowners. Cyber insurance also will impose some realignment/restructuring of insurance organizations. Carriers not willing to address the changes needed to properly service customers' growing cyber risk needs may find themselves out of the market altogether. CM

David Pieffer *is the Property & Casualty Insurance Practice Lead for J.D. Power, where he handles advancing the growth of J.D. Power's core P&C insurance practice.*