Rich Sheridan, Chief Claims Officer, Berkley Cyber Risk Solutions

FEASTING ON CYBER DATA

While cyber losses wreak havoc on one end, they provide a slew of data that carriers need for better products and proper pricing.

As a newer and developing area of insurance, cyber is a field where a paucity of data has cramped insurers' ability to analyze exposures. As the sector matures and carriers make more payments under their policies, claims departments are gathering data that reveal what is driving cyber liability costs. The compilation of data is helping insurers better predict and control those costs.

As in other areas of insurance, cyber claims departments track losses by industry or sector. While some events are widely publicized and provide very public sources of loss data—recall the 2013-2014 credit card exposures at major retailers—individual carriers have been able to measure cyber losses in other, lower-key sectors using their own, proprietary claims data.

Carriers are also tracking cyber losses by cause of loss. For instance, cyber policies can be triggered as the result of lost laptops, hacking incidents, lost paper documents or a variety of other causes. New causes of loss are constantly evolving, however. Three years ago, most people had never heard of a W-2 phishing event—a scenario where an impostor pretending to be an executive or other person within a company induces an employee to email the W-2 forms of the company's employees. Yet this type of event has been a common occurrence over the last two years. When I think how quickly previously unknown types of cyber losses become commonplace, I WannaCry.

Breach response costs under both first- and third-party coverages are also under scrutiny. Covered first-party expenses may include costs for legal breach counsel, forensics, notification and credit monitoring, public relations, data restoration, business interruption and ransomware response. Naturally, carriers are tracking how much is being spent for each of these specific types of breach response costs. But just as we are continually seeing new causes of loss under cyber insurance policies, we are also seeing new or expanded types of coverage. For instance, business interruption is a relatively new coverage offered by cyber carriers, who are of course interested in tracking those costs as well the expenses that go along with this coverage, like the cost to retain forensic accountants. Until cyber policies started offering business interruption coverage, there was little desire or need to track the costs incurred by forensic accountants—no such costs were being incurred!

Carriers are getting more certainty as to the costs that may be incurred under cyber policies by pre-negotiating rates with breach response vendors. Moreover, some breach response vendors help carriers track these costs. At least one breach notification vendor tracks the "take rate"—the percentage of individuals who have been notified that their personal information has been exposed in a data breach who then apply for credit monitoring. The number of people phoning into call centers following data breaches is also tracked. This information is grouped by industry and by type of data, so now carriers can, for instance, get a better idea of how many people may seek credit monitoring when a retailer suffers a credit card hacking/breach incident and, more importantly, better project the cost of providing those services.

Aside from tracking actual incurred costs, some vendors provide services that increase cost certainty. For instance, multiple forensic vendors now handle ransomware extortion matters, where an entity's computer system is frozen or locked by malware, for a flat fee (plus the ransom amount). The extorters typically seek a ransom in the form of bitcoin or some other virtual currency, and for this flat fee, the forensics vendor will obtain the bitcoin, contact the extortionist, obtain the "key" to unlock the system, and analyze the system to make sure that the malware has been removed.

The development of claims over the last several years has allowed cyber carriers to make great progress in their ability to analyze cyber exposures. This remains a work in progress, however, and claims departments need to remain diligent as to what will develop in this area of insurance, whether it be a wave of ransomware attacks, an industry sector showing increased vulnerability, or some as yet unknown area of focus. ■

Berkley Cyber Risk Solutions is a member company of W. R. Berkley Corporation, a Fortune 500 company. The views expressed herein are solely those of the author and do not necessarily represent the views of W. R. Berkley Corporation.