Commissioner's Column

Cybersecurity and the Future of Insurance

April 2018

To find proof that there's nothing new under the sun, I only have to look back into the past editions of my column. Three years ago, in March of 2015, I was sounding the alarm about cyberattacks, most notably at the time the attack on Anthem, Inc. Here again, I feel the need to spread the word about cybersecurity attacks. Not just their frequency, which seems to be happening so often that small-scale attacks are getting less and less attention, but the changing landscape of what cybersecurity has become.

Threats to data privacy are nothing new. Regulators and legislatures have required businesses to protect consumer data for decades. However the modern size, scale and methods of data collection, transmission and storage all present new challenges. As we become more reliant on electronic communication and businesses collect and maintain ever more granular information about their customers, the opportunity for bad actors to inflict damage on consumers and businesses increases exponentially. In addition to large scale hacking like in the case of 145 million American consumers who had their personal information stolen from Equifax, there have been cases of hackers locking information away from businesses and then ransoming access back.

Already this year, a hospital in Indiana faced the difficult choice of paying a ransom or having hackers delete their patient data. The hackers replaced all information in thousands of patient records with the words "I'm sorry" and demanded four bitcoins, valued at $55,000 at that time, in return for releasing the data. Faced with possible weeks of reconstructing data on their own should the information be erased, the hospital paid the ransom. There are more stories of the same sort from around the country. The amounts are usually strategically lower than it would cost for the hostage company to fix the problem on their own.

There's a lot of room for improvement in this sector. Most businesses are familiar with commercial insurance policies that provide general liability coverage to protect against injury or property damage. What they may not realize is that most standard commercial lines policies do not cover many cyber risks – and they must secure a special cybersecurity policy. Aon Benfield estimates that less than 15 percent of US businesses have cybersecurity insurance and less than one percent in other regions of the world. In fact, Aon Inpoint estimated the global standalone cyber market to be worth $1.7 billion in annual gross written premium in a study conducted in 2015.

While the need for cybersecurity insurance for businesses is large, cybersecurity risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data. In the absence of such data, insurers compensate with pricing that relies on qualitative assessments of an applicant's risk management procedures and risk culture. As a result, policies for cyber risk tend to be more customized than policies for other risks, and therefore more costly. There are many factors that go into determining the scale and cost of a policy including the type of business operation seeking coverage, the size and scope of operations, the number of customers, the type of data collected and how it is stored.

From a regulatory perspective, we would like to see insurers use quantitative measures like those listed above coupled with robust actuarial data based on actual incident experience. To aid in collecting this data and protecting consumers, the National Association of Insurance Commissioners (NAIC) adopted the Insurance Data Security Model Law in late 2017. That model establishes the standards for data security and investigation and notification of a breach of data security applicable to insurance providers.

In a constantly connected world, we are all vulnerable to this sort of attack on our businesses and personal data. At the Department of Insurance, we are committed to working with companies to keep their data and consumer personal information as safe as possible. All of us working together can provide a united front, faster responses and stronger defenses against those who will attempt to use illegal hacking for their own gains.