American Academy of Actuaries
Essential Elements
Making complex public policy issues clear
DECEMBER 2016

Managing the Risks in Cyberspace

A growing number of large retailers, insurers, government agencies, and other organizations are reporting cyberattacks that attempt to steal personal data.[1] Hackers also have taken trade secrets or damaged networks with malicious computer software after gaining access to organizations' computer networks. One response has been more businesses and individuals seeking protection through a cyber-risk insurance policy, which has become an emerging line of business. A cyberattack on a single business could affect thousands of businesses or millions of consumers.

Protecting Insurer Data

Insurers, particularly those in the health care field, make tempting targets for hackers because they house large amounts of consumer data, ranging from Social Security numbers and employment data to details about family members. Health insurer Anthem suffered a major data breach in 2015 that exposed information from 79 million customers, and many other insurers have had their company information compromised as well.

Cyber-Risk Insurance

Besides protecting their policyholder and other proprietary data, some insurers offer private insurance coverage of certain cyber-risks, such as the hacking into computer networks by outside parties either with political motivations or seeking to profit, accidental or intentional release of sensitive data by employees, and physical damage or business disruption.

While relatively new, the market for cyber-risk insurance coverage is expected to grow rapidly. Nearly $484 million for standalone cybersecurity policies and about $1 billion in cybersecurity package policies were written in 2015, according to an NAIC survey of 500 insurers.[2]

Most standard commercial policies do not insure against many cyber-risks, and businesses that seek such coverage must purchase special policies that could cover:

- Theft of customer lists, trade secrets, and other valuable private data
- Business interruption damages from a cyberattack
- Damages caused by introduction of malicious computer software
- Costs from employees who accidently or maliciously disclose sensitive business information
- Costs of complying with state and federal data-breach laws
- Reputational damage

Cybersecurity also affects personal lines of insurance, and some homeowner's policies now offer identity theft protection. Automobiles are increasingly dependent on computer technology, which could be vulnerable to hacking. Other at-risk household items include so-called smart thermostats, wireless-enabled front door locks, and

1 *The Global State of Information Security® Survey 2017*; PwC; 2016.
2 "Early NAIC Analysis Sheds Light on Cybersecurity Insurance Data;" National Association of Insurance Commissioners; June 30, 2016.

American Academy of Actuaries
Objective. Independent. Effective.™
1850 M Street NW • Suite 300 • Washington, DC 20036 • 202.223.8196 • www.actuary.org

appliances that are connected to the internet and to each other.

Within auto or property insurance companies, substantial data exists on accidents, and actuaries can calculate the risks, prices, and reserves necessary. However, there is far less data on cyber-risks because data breaches are relatively new, which makes calculating prices and reserves more difficult. Insurance prices set too high will limit the number of businesses that find coverage economical or individuals who can afford coverage, while prices that are too low could lead to insurers not being able to pay all claims.[3]

Recent Major Data Breaches

COMPANY	POTENTIAL USERS	YEAR
Weebly	43 million	2016
Verizon	1.5 million	2016
Anthem	79 million	2015
Securus Technologies	70 million	2015
Yahoo!	500 million	2014
eBay	145 million	2014
JPMorgan Chase	76 million	2014
Home Depot	56 million	2014

Because personal and commercial cyber-risk coverage is evolving, most policies are being created uniquely for each policyholder in order to define the circumstances that trigger payouts. Insurers that write commercial cyber-risk policies typically will review companies' antivirus and malware-protection software, frequency of system and software updates, and performance of firewalls. Insurers also will analyze how a company's employees, vendors, and customers access data, especially those having access to critical data. Another key area is a firm's post-breach response plan as it relates to the risk management of its networks, websites, and intellectual property.

New Policies and Regulations

Because cybercrime is a growing threat, various government entities are taking steps to reduce the risks. Congress passed the Cybersecurity Act of 2015, a law that creates a mechanism for data sharing among companies and federal agencies, authorized various government and non-government entities to monitor certain information and take defensive measures for cybersecurity purposes, and contained provisions to strengthen cybersecurity protections at federal agencies.

State insurance regulators have monitored breached companies and receive input from law enforcement to ascertain what insurers are doing to take appropriate steps to protect data. The National Association of Insurance Commissioners (NAIC) has taken a leading role in addressing cyber-risk in the insurance industry, and has:

- Released principles of best practices for insurers and regulators on protecting insurers' data from hacking.
- Established a roadmap[4] of cybersecurity protections for consumers in cases of data breaches that include: notices from insurers in cases of identity theft, one year of identity theft protection paid for by insurers, and the right to place a 90-day initial fraud alert on credit reports.
- Collected reports for analysis from more than 500 insurers that have provided businesses and individuals with insurance for cyber-risks through policies that mainly were additions to commercial and personal policies.
- Started drafting a model law for state legislatures to consider. Provisions in the model law include requirements on insurers to: implement information security programs; and investigate and notify regulators, consumers, affected payment card companies, and consumer-reporting services about data breaches.

Conclusion

While insurers provide coverage for many types of risks, there currently is limited data to analyze on cyber-risks, which involve complex technologies that are constantly changing. Additionally, cyberattacks involve new targets, threats, and perpetrators. These changes limit the usefulness of historical data for predicting future costs of cyber-risks. U.S. businesses and consumers have become increasingly reliant on computer technology, and insurers and regulators are trying to catch up with the ensuing cyber-risks.

3 Testimony by North Dakota Insurance Commissioner Adam W. Hamm before the U.S. House Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies; March 22, 2016.

4 "NAIC Roadmap for Cybersecurity Consumer Protections"; NAIC and the Center for Insurance Policy and Research; 2015.