April 2017

GOVERNMENT RELATIONS
ISSUE BRIEF

700 HALL OF STATES
444 NORTH CAPITOL STREET N.W.
WASHINGTON, D.C. 20001
202-471-3990
www.naic.org

NAIC
National Association of Insurance Commissioners
& The Center for Insurance Policy and Research

Cybersecurity: Protecting Insurance Consumers in a Digital Age

- *State insurance regulators are keenly aware of the potentially devastating effects cyber-attacks can have and continue to develop and improve privacy protections and data security safeguards that focus on the security and confidentiality of consumers' sensitive non-public personal and health information.*

- *The NAIC updated its cybersecurity examination protocols to better ensure that insurance companies are adequately protecting consumer data. NAIC is also working to develop an Insurance Data Security Model Law that establishes standards for data security, investigation, and data breach notification that will create certainty for insurance consumers and licensees.*

- *State insurance regulators are also closely monitoring the growth of the cyber liability insurance market, gathering and analyzing financial data, engaging with carriers and reviewing regulatory requirements pursuant to the marketplace.*

Background

Insurance companies, agents, and brokers retain highly sensitive consumer financial and health information for legitimate business reasons including underwriting insurance risks and evaluating and paying policyholder claims. State insurance regulators have taken a number of steps to enhance data security expectations to ensure these entities are adequately protecting this information. As part of these efforts, the NAIC developed Principles for Effective Cybersecurity that set forth the framework through which insurance regulators will evaluate efforts by insurers, producers, and other regulated entities to protect consumer information entrusted to them. The NAIC also adopted a Roadmap for Consumer Cybersecurity Protections to describe protections state insurance regulators believe consumers should be entitled to from insurance companies and agents when these entities collect, maintain, and use personal information and to guide ongoing efforts in developing regulatory guidance for insurance sector participants.

The NAIC reviewed and updated cybersecurity examination standards in the NAIC Financial Examiner's Handbook to incorporate concepts from the NIST Cybersecurity Framework, and similar enhancements are expected to be made to the NAIC Market Conduct Examiner's Handbook. The NAIC also adopted a new Cybersecurity and Identity Theft Insurance Coverage Supplement to the Property and Casualty Annual Statement to gather information about the insurers selling cybersecurity insurance products and the market for such products. The NAIC released a report in August 2016 regarding the results of the first filing of the cybersecurity supplement, which indicates that more than 500 insurers have provided businesses and individuals with cybersecurity insurance. State insurance regulators will continue to collect this data in order to perform trend analysis on exposures, premium volumes, and claims activities moving forward.

Other Key Points

- ✓ Cybersecurity is a top priority for state insurance regulators, who understand it as a critical part of enterprise risk management.

- ✓ State insurance regulators continue to implement and upgrade safeguards to protect the security, confidentiality, and integrity of customer information through standards, the examination processes, and model laws in this area.

- ✓ Congressional activity on cybersecurity should not disregard the existing state regulatory framework and should not inhibit ongoing efforts in the states to develop laws and regulations in the best interests of consumers.

Ethan Sonnichsen, Managing Director, Government Relations esonnichsen@naic.org
Mark Sagat, Assistant Director, Financial Policy and Legislation msagat@naic.org
Brooke Stringer, Financial Policy and Legislative Advisor bstringer@naic.org