Deciphering cybersecurity: introduction to cybersecurity regulatory initiatives in insurance industry

MAYER • BROWN

20 November 2018 | Contributed by Mayer Brown LLP

Insurance, USA

Introduction

The past five years have seen a massive acceleration in the amounts of data being generated, processed and stored in virtually every industry, including insurance. As with most industries, insurance data increasingly resides in flexible networks, utilising, for example, virtual machine storage, which allows for increased accessibility by support staff and consumers. While doubtlessly providing benefits for insurance companies and producers on an operational level, such flexibility comes at a price, as such practices also expose data to increased security threats. It should therefore come as no surprise that there has been a growing trend of increasingly sophisticated cyberattacks which have, in many ways, outpaced current data security technology. In recent years, major financial institutions and retailers have all been the unfortunate victims of such cyberattacks – and the insurance sector has been by no means immune from this trend, with large-scale attacks against large health insurers being perhaps the most visible data breaches in the insurance sector.

The consequences of data breaches are particularly pronounced in the insurance industry, where insurers and insurance producers are custodians of highly sensitive information, including personal financial and health information obtained as part of their services to consumers. It is no exaggeration to conclude that developing a coherent cybersecurity strategy is one of the most important challenges facing insurance industry participants today.

US regulation

In the United States the business of insurance is regulated primarily at the state level, which means that industry participants who operate on a nationwide basis need to comply with the regulatory requirements of each of the 50 states and the District of Columbia. Among state insurance regulators, the New York Department of Financial Services has been notable for issuing a wide-ranging cybersecurity regulation which impose strict data security requirements on participants in the New York insurance market.

On the national level, concerns about cybersecurity have received significant attention. In February 2014 the Department of Commerce's National Institute of Science and Technology (NIST) issued a framework to guide cybersecurity improvements for critical infrastructure. The framework sets out standards, guidelines and practices to structure effective ways of managing cyber risks.

Subsequent to the NIST initiative, the National Association of Insurance Commissioners (NAIC) acted in a similar vein in April 2015, adopting 12 principles for effective cybersecurity to provide a foundational tool for state insurance regulators to develop their own guidance for protection of their respective insurance sector's data security and infrastructure.

Model law

In October 2017 the NAIC went a step further and adopted an Insurance Data Security Model Law. The model law is a major initiative by the NAIC to respond to public concerns of the inadequacy of current cybersecurity regulation and legislation to combat the various risks presented by cyberattacks. The NAIC model law establishes a legal framework for requiring insurers and insurance producers to operate complete cybersecurity programmes, including planned cybersecurity testing and upper management involvement in the information security programme, as well as incident response plans and specific breach notification procedures. Although it is only a model law (and, consequently, not enforceable unless and until it is approved and adopted by individual states), the NAIC has an aggressive goal of encouraging legislatures or regulatory bodies to adopt the model law, with as few changes as possible, in a majority of states within three years. In addition, once a particular state adopts the model law, insurers in such state will only have one year to comply with most of the model law's requirements. The NAIC model law, while similar in many respects to the New York cybersecurity regulation, also includes additional guidelines, including with respect to board involvement in a company's information security programme and detailed event reporting requirements. On 3 May 2018 South Carolina became the first state to enact the NAIC model law and legislation to enact the model law was introduced earlier this year in Rhode Island but has not yet passed. It is expected that similar bills to enact the model law will be introduced in additional states in 2019.

Comment

The NAIC's Insurance Data Security Model Law has been well received at the federal level, with the Department of the Treasury, in its October 2017 Report on Asset Management and Insurance, openly endorsing the model law and recommending that Congress consider adopting federal legislation that would pre-empt state law if the model law is not adopted within five years. Accordingly, it is clear that the topic of cybersecurity will remain a crucial topic for the insurance sector in the years to come.

For further information on this topic please contact at Lawrence R Hamilton at Mayer Brown LLP's Chicago office by telephone (+1 312 782 0600) or email (lhamilton@mayerbrown.com). Alternatively, contact Sanjiv Tata at Mayer Brown LLP's New York office by telephone (+1 212 506 2500) or email (stata@mayerbrown.com). The Mayer Brown LLP website can be accessed at www.mayerbrown.com.

The materials contained on this website are for general information purposes only and are subject to the disclaimer.

Lawrence R Hamilton

Sanjiv J Tata