MAYER | BROWN

@Insurance Snapshot.
Technology & Innovation News & Views

October 5, 2018

Deciphering Cybersecurity: An Introduction to Cybersecurity Regulatory Initiatives in the Insurance Industry

By Larry Hamilton and Sanjiv Tata[1]

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, utilizing, 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.

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 twelve 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.

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 cyberattack. The NAIC model law establishes a legal framework for requiring insurers and insurance producers to operate complete cybersecurity programs, including planned cybersecurity testing and upper management involvement in the information security program, 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. Additionally, 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 program and detailed event reporting requirements. On May 3, 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. We expect to see similar bills to enact the model law introduced in additional states in 2019.

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 preempt state law if the model law is not adopted within 5 years. Accordingly, one can expect that the topic of cybersecurity will remain a crucial topic for the insurance sector in the years to come.

Endnotes

[1] Larry Hamilton leads Mayer Brown's US insurance regulatory practice within the Insurance Industry group. He advises insurance companies, insurance agencies and investment companies on a broad range of regulatory matters, including those associated with formation, licensing, portfolio investments, reinsurance, e-commerce, cybersecurity and outsourcing. He is also a member of Mayer Brown's Cybersecurity & Data Privacy practice. Sanjiv Tata is an associate in Mayer Brown's New York office and a member of the Corporate & Securities practice, specializing in insurance regulatory work. Sanjiv advises insurance companies, insurance intermediaries and investment companies with respect to a broad range of insurance regulatory and corporate matters, including formation and licensing of insurance companies, mergers and acquisitions of insurance companies, reinsurance transactions, and enforcement, corporate governance, cybersecurity, enterprise risk and general compliance matters.

Mayer Brown is a distinctively global law firm, uniquely positioned to advise the world's leading companies and financial institutions on their most complex deals and disputes. With extensive reach across four continents, we are the only integrated law firm in the world with approximately 200 lawyers in each of the world's three largest financial centers—New York, London and Hong Kong—the backbone of the global economy. We have deep experience in high-stakes litigation and complex transactions across industry sectors, including our signature strength, the global financial services industry. Our diverse teams of lawyers are recognized by our clients as strategic partners with deep commercial instincts and a commitment to creatively anticipating their needs and delivering excellence in everything we do. Our "one-firm" culture—seamless and integrated across all practices and regions—ensures that our clients receive the best of our knowledge and experience..

Please visit mayerbrown.com for comprehensive contact information for all Mayer Brown offices.

Any tax advice expressed above by Mayer Brown LLP was not intended or written to be used, and cannot be used, by any taxpayer to avoid U.S. federal tax penalties. If such advice was written or used to support the promotion or marketing of the matter addressed above, then each offeree should seek advice from an independent tax advisor.

This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively the "Mayer Brown Practices") and non-legal service providers, which provide consultancy services (the "Mayer Brown Consultancies"). The Mayer Brown Practices and Mayer Brown Consultancies are established in various jurisdictions and may be a legal person or a partnership. Details of the individual Mayer Brown Practices and Mayer Brown Consultancies can be found in the Legal Notices section of our website.