NAIC Adopts Model Law on Cybersecurity: Will the States Adopt?

Christopher M. Brubaker

December 26, 2017

On October 24, 2017 the National Association of Insurance Commissioners ("NAIC") formally approved the Insurance Data Security Model Law ("Model Law"). The NAIC is a standard setting and regulatory support organization consisting of the top insurance regulators from the 50 states, District of Columbia, and five U.S. territories. The Model Law applies to "Licensees" which are defined as persons and non-governmental business entities subject to the insurance laws of the State adopting the Model Law. (Model Law, § 3(I). Unless otherwise defined herein capitalized terms are defined in the Model Law.) In Pennsylvania, for example, this would encompass insurance companies and insurance producers (i.e. agents, agencies, and brokers). Notably, this applies to non-resident Licensees except for purchasing groups, risk retention groups, or when acting as assuming insurer. (Id.) For example, a broker resident in a state that has not adopted the Model Law, is potentially subject to the Model Law if they are also licensed in another state that has adopted the Model Law. Thus, it will be important to track what states enact the Model Law and also how uniformly the Model Law is enacted state to state.

The intent of the Model Law is to establish standards for data security, the investigation of Cybersecurity Events, and notification of the Commissioner of Cybersecurity Events. (Model Law, § 2(A).) In order to understand how the Model Law attempts to meet those objectives it is necessary to understand how the Model Law has defined the different elements that are involved in cybersecurity. A Cybersecurity Event is defined as "an event resulting in unauthorized access to, disruption or misuses of, an Information System or information stored on such Information System." (Model Law, § 3(D).) Information System is defined broadly as "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information…" and expressly includes "specialized systems such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems." (Model Law, § 3(H).) This broad definition encompasses both traditional computer networks and devices, but also other machines that fall under the rubric "the internet of things" and systems such as HVAC systems which have been the entry point for hackers in notable data breaches. Information Security Program means "the administrative, technical and physical safeguards that a Licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Nonpublic Information."

Nonpublic Information is defined more broadly than most data breach notification laws and includes business related information of the Licensee the disclosure of which could cause a material adverse impact on the Licensee's business, operations, or security. (Model Law, § 3(K)(1).) Nonpublic information also includes any information about a Consumer which can be used to identify the Consumer in combination with any one or more of Social Security number, driver's license or other identification number, account number, credit or debit card number, security code, access code, or password to a financial account, or biometric records. (Model Law, § 3(K)(2).) Nonpublic information also includes any data other than age and gender

derived from a health care provider or the Consumer related to the Consumer's past, present, or future physical, mental, or behavioral health or condition or that of the Consumer's family. (Model Law, § 3(K)(3).) Publicly Available Information means any information that a Licensee has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records; widely distributed media; or, disclosures to the general public required by federal, state, or local law. (Model Law, § 3(M).)

The Model Law requires Licensees to implement a comprehensive written Information Security Program based on the Licensees' Risk Assessment. (Model Law, § 4(A).) As part of the Information Security Program the Licensee must designate an individual (who can come from a third-party) to be responsible for the Information Security Program. (Model Law, § 4(C)(1).) The Risk Assessment must identify reasonably foreseeable internal and external threats to Nonpublic Information including any Information Systems or Nonpublic Information that are controlled or accessible by Third-Party Service Providers; assess the likelihood and severity of damage by these potential threats; assess the sufficiency of existing policies, procedures, and technology in place to protect against such threats; and, implement information safeguards to manage the identified threats and at least annually assess their effectiveness. (Model Law, § 4(C)(2)-(5).) The Model Law puts special emphasis in assessing the Licensees' policies, procedures, Information Systems and safeguards with respect to: employee training and management; Information Systems including information classification, governance, processing, storage, transmission and disposal; and, detecting, preventing, and responding to attacks, intrusions, or other system failures. (Model Law, § 4(C)(4).)

The Model Law also mandates that Licensees perform continuing risk management with respect to cybersecurity issues. (Model Law, § 4(D).) A Licensee, commensurate with its size and complexity of activities, shall design its Information Security Programs to mitigate the risk identified in the Risk Assessment. (Model Law, § 4(D)(1).) At a minimum a Licensee must evaluate the appropriateness of implementing eleven enumerated security measures including implementing access controls with authentication on Information Systems, restricting access at physical locations with Nonpublic Information, encryption, and to regularly test and monitor systems and procedures to identify actual and attempted attacks or intrusions. (Model Law, § 4(D)(2).) Licensees must also include cybersecurity risks in their enterprise risk management process, stay informed regarding emerging threats and vulnerabilities, and provide its personnel with cybersecurity awareness training as necessary to reflect risks identified in the Risk Assessment. (Model Law, § 4(D)(3)-(5).) The Model Law also mandates oversight of the Information Security Program by a Licensee's board of directors, if applicable. (Model Law, § 4(E).) Other responsibilities include oversight of Third-Party Service Providers, ongoing monitoring, evaluation, and adjustment as necessary of the Information Security Program, establishment of a written incident response plan, and annual certification of compliance with section 4 to the (insurance) Commissioner. (Model Law, § 4(F)-(I).)

The Model Law also contains detailed provisions regarding the investigation of and notification regarding Cybersecurity Events. (Model Law, §§ 5 and 6.) Licensees must investigate whenever there is or may have been a Cybersecurity Event. (Model Law, § 5.) The investigation can be performed by an outside vendor on behalf of the Licensee. (Model Law, § 5.) There are separate notification requirements for the Commissioner, Consumers and

reinsurers. (Model Law, § 6.) The Commissioner also has the authority to investigate Licensees' compliance with the Model Law and to take action to enforce the Model Law. (Model Law, § 7.) Importantly, the Model Law provides for confidentiality of information provided pursuant to a Licensee's annual certification under section 4(I) and much of the information that must be reported to the Commissioner following a Cybersecurity Event under section 6, and investigations under section 7. (Model Law, § 8.) The Model Law expressly provides that these documents are not subject to freedom of information act or similar laws, subpoenas, or discovery in civil actions and are inadmissible in civil actions. (Model Law, § 8.) The Commissioner is authorized to use such documents as necessary in any action or proceeding it institutes to enforce the Model Law under section 7. (Model Law, § 8.) There is an exception for Licensees with fewer than ten employees, including independent contractors, and individual Licensees who are covered by the Information Security Program of another Licensee. (Model Law, § 9(A)(1) and (3).) In addition, Licensees subject to HIPPA that have established and maintain Information Security Programs pursuant to HIPPA are deemed to be in compliance with section 4. (Model Law, § 9(A)(2).) In section 10 the Model Law contemplates penalties for non-compliance in accordance with the enacting state's general penalty statute. (Model Law, § 10.) Section 11, which is noted as optional allows for the implementation of additional rules and regulations necessary to carry out the provisions of the Model Law. (Model Law, § 11.)

The Model Law is similar, but not identical, in structure and scope to New York's recent cybersecurity rules applicable to Banks, Insurance Companies and other Financial Services Companies, 23 NYCRR 500 ("NY Cyber Rules"). The Model Law contains a Drafting Note indicating it is the drafters' intent that if a Licensee is in compliance with the NY Cyber Rules then the Licensee is in compliance with the Model Law. Like the NY Cyber Rules the Model Law is based on a risk assessment or risk management approach to cybersecurity. This approach is widely regarded as a best practice in terms of approach to cybersecurity. What is still very much in question is the ability of regulations of this type to actually improve cybersecurity. As both the Model Law and NY Cyber Rules tacitly acknowledge there is no perfect answer or approach to cybersecurity. Security measures necessary and appropriate for large companies will often not fit smaller companies and vice versa. Examples include the frequency and sophistication of penetration and other testing methods and the scope and intensity of employee training. Further, it is widely accepted by security experts that everybody is vulnerable no matter how rigorous their cybersecurity is. Can regulations effectively improve cybersecurity in this type of risk environment? We shall see.

Another critical hurdle facing the Model Law that will greatly impact how effective it is in improving cybersecurity, is how widely and uniformly it is adopted by states. These are issues that often plague model laws regardless of subject and there are numerous examples of limited adoption, lack of uniformity of adoption, or both in existing model laws. Penalties and enforcement are another area that could potentially vary greatly state to state. The NAIC looks to have come up with a fairly balanced approach to cybersecurity regulation and companies large and small would be wise to follow many of the processes and procedures required by the Model Law. But there are many open questions surrounding the Model Law the answers to which will determine its success at improving cybersecurity in the insurance industry and as a model for other industries to follow.

Christopher M. Brubaker of Clark Hill concentrates his practice in complex commercial litigation and insurance matters. He regularly provides advice to companies on insurance and cyberrisk issues related to transactions and risk management and also advised companies on regulatory matters involving insurance and environmental laws, rules and regulations. He frequently speaks and writes on cybersecurity matters for legal and professional groups.