South Carolina Adopts NAIC Cybersecurity Model Law

Michael A. Molony	**T. Douglas Concannon**	**Leslie M. Whitten**
YCR Law	YCR Law	YCR Law
843.724.6632	843.724.6640	843.724.6691

On May 9, 2018, South Carolina Governor Henry McMaster signed into law the South Carolina Insurance Data Security Act ("**IDSA**"). South Carolina thereby became the first state in the nation to pass legislation modeled after the "Insurance Data Security Model Law" adopted by the National Association of Insurance Commissioners ("**NAIC**"). The purpose of the IDSA is to ensure that all Licensees of the South Carolina Department of Insurance ("**SC DOI**") have a strong and aggressive cyber security program to protect the personal data of consumers in South Carolina and elsewhere.

To Whom Does the IDSA Apply?

The IDSA broadly applies to all "licensees" of the SC DOI, including "any [individual or corporate] person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State." The ISDA applies to both resident and non-resident insurers, agencies, producers, and brokers. It expressly excludes only (1) out of state purchasing groups or risk retention groups and (2) out of state licensees who are acting only as an assuming reinsurer.

What Does The ISDA Require?

The ISDA became effective January 1, 2019. It includes several staggered effective dates for implementation of its requirements.

- Beginning Immediately: Licensees must comply with the reporting requirements of a Cybersecurity Event.

  Under the Act, a "Cybersecurity Event" is defined as "an event resulting in an unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System." "Cybersecurity Event" does not include the unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released or used without authorization. "Cybersecurity Event" does not include an event with regard to which the Licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed. Loss of information only in paper format does not constitute a "Cybersecurity Event."

  Licensees must notify the SC DOI within 72 hours after determining that a Cybersecurity Event has occurred if (1) South Carolina is the Licensee's domicile; or (2) the Licensee is not domiciled in South Carolina, but it is reasonably believed to have involved the release of the nonpublic information of 250 or more South Carolina consumers and the Cybersecurity Event impacts the Licensee such that notice must be provided to another state or federal government entity, or there is a reasonable likelihood of material harm to a South Carolina consumer or material parts of the Licensee's operations.

- Beginning July 1, 2019: Licensees must have an IS Program.

  Licensees have until July 1, 2019 to develop, implement, and maintain a comprehensive written information security program ("**IS Program**") that provides protection for nonpublic information and the Licensee's information systems.

  The ISDA establishes broad requirements for a compliant IS Program. The IS Program must be commensurate with the size and complexity of the licensee, the nature and scope of its activities, and the sensitivity of the nonpublic information that is in its control, either directly or through third-party providers. The ISDA does not require the use of specific cybersecurity frameworks. Instead, it requires that the IS Program must contain "administrative, technical, and physical safeguards" for the protection of nonpublic information. It also

includes an extensive list of standard definitions and general requirements, as well as details that must be included for an IS Program to be deemed compliant.

As outlined above, the Licensee's IS Program must include a written incident response plan designed to promptly respond to or recover from any Cybersecurity Event. The Act contemplates that the Licensee will notify the SC DOI as soon as it is confirmed that there was unauthorized access, misuse, or disruption to nonpublic information from the Licensee's information system or that of the Licensee's third-party service provider. Licensees have a continuing obligation under the law to update initial and subsequent notifications to the Director concerning the Cybersecurity Event. Licensees will not be required to notify the Department of temporary disruptions in service due to power outages or other benign causes unless the disruption results in the unauthorized access, misuse, or disruption of the Licensee's information system or that of its third-party service provider.

- Licensees have until July 1, 2020 to ensure their third party service providers have implemented and are maintaining a compliant IS Program.

What Else Does the ISDA Address?

Exemptions. The following Licensees are exempt from having to develop their own information security program:

- Those with fewer than 10 employees;
- Employees, agents, representatives, or designee of a licensee to the extent that person is covered by the information security program of another licensee;
- Those able to certify compliance with the requirements of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and which have established and maintain an information security program pursuant to those requirements; and
- Licensees that are subject to and able to certify compliance with the New York cybersecurity regulation.

However, these *exempted Licensees must still comply with other provisions of the IDSA*. Qualifying for an exemption does not remove a Licensee from the duty to protect data and nonpublic information under other state and federal laws, like the Graham Leach Bliley Act and Fair Credit Reporting Act. In the event a Licensee ceases to qualify for one of the exemptions listed above, the Licensee must develop a compliant information security program within 180 days.

Corporate Governance. The ISDA provides minimum requirements for a Licensee's Board of Directors regarding the Board's oversight responsibilities for the IS Program, as well as specific details regarding third-party risk management requirements.

Continual Updating. Licensees are required to perform annual risk assessments to evaluate the effectiveness of key controls, systems, and procedures, and must submit an annual certification to the state's insurance commissioner certifying that the company is in compliance with all of the ISDA's requirements. Depending on the findings of the risk assessment, Licensees must implement appropriate security measures such as access and authentication controls, physical access restrictions, encryption, testing and monitoring of systems to detect attacks and intrusions, and measures to protect against the destruction, loss, or damage of such information.

Annual Certification. Beginning February 15, 2020, insurers domiciled in South Carolina will need to submit an annual written statement to the SC DOI certifying their compliance with the data security program requirements.

Confidentiality. Particularly given the subject of the ISDA and the nature of its requirements, it is important to note that the ISDA provides that documents, materials, and other information in the control or possession of the SC DOI obtained in an investigation or examination must be treated as confidential and privileged, but the SC DOI may use such information in furtherance of regulatory action and share or receive confidential documents under certain circumstances.

Enforcement. Not surprisingly, the ISDA grants the SC DOI authority to examine and investigate a Licensee's compliance and provides penalties for violations of the ISDA. Rather than spelling out specific penalties for different violations, the ISDA instead defers to South Carolina's existing general insurance penalty statutes. If the violator is an insurer, it could be subject to a fine in an amount up to $15,000 per violation, and suspension or revocation of the violator's authority to do business in the state. Other persons risk a fine in an amount up to $2,500 per violation, and suspension or revocation of the violator's license. These fine amounts automatically double if the violation is found to be willful.

The ISDA also authorizes the SC DOI to promulgate regulations necessary for the administration of the Act. The Director of Insurance already has outlined a reporting process and promulgated a reporting form to simplify the reporting requirements for Licensees in the event of a Cybersecurity Event. SC DOI Bulletin 2018-09. The SC DOI is working closely with the NAIC in an effort to ensure consistency among the states as the ISDA and other variations of the NAIC model law are put into practical effect.

Conclusion

South Carolina's adoption of the NAIC Insurance Data Security Model Law is part of a broader trend that has seen regulatory requirements related to cybersecurity become increasingly specific and far-reaching. The overall goal of an IS Program – and of IT risk management in general – is to provide for the confidentiality, integrity, and availability of information assets. Typically, this involves numerous complex and highly interrelated components. Regulatory compliance is only one of them. Virtually all insurance-related businesses should already be making plans and studying what other regulated industries have done to adopt effective cybersecurity measures.