Client Alert: Ohio's New Cybersecurity Requirements on Insurers and Other Licensees Set to Take Effect in March

Related Professionals

Anthony Spina

John L. Landolfi

Christopher L. Ingram

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 2.18.2019

Ohio recently added comprehensive cybersecurity requirements to its insurance laws through Substitute Senate Bill 273 (the Ohio Cybersecurity Law), which take effect on or about March 19, 2019 (the Effective Date). The Ohio Cybersecurity Law is based on, with some modifications, the Insurance Data Security Model Law adopted by the National Association of Insurance Commissioners. Ohio joins South Carolina and Michigan in recent adoptions of the model law.

Ohio's Cybersecurity Law is applicable to any person under Ohio's insurance laws who is licensed, authorized, or registered to operate, or required to be licensed, authorized, or registered to operate, which includes insurance companies (Licensees). However, Licensees with less than twenty employees, less than five million dollars in gross annual revenue, or less than ten million dollars in assets are exempt from the law.

On the heels of high-profile data breaches in the insurance industry, the law establishes broad data security requirements and imposes standards for investigating and reporting data security incidents. Licensees have one year to comply with most of the new cybersecurity requirements. Importantly, the law represents the "exclusive state standards and requirements applicable to licensees regarding cybersecurity events, the security of nonpublic information, data security, investigation of cybersecurity events, and notifications to the superintendent of cybersecurity events." R.C. § 3965.09.

The Ohio Cybersecurity Law will have a significant impact on the operations and corporate governance of Licensees. For example, it requires Licensees to:

Adopt a Written Cybersecurity Program

Each Licensee is required to develop, implement and maintain a comprehensive written information security program based upon the Licensee's own risk assessment (the Security Program). The Security Program should be commensurate with the size and complexity of the

Licensee, the nature and scope of the Licensee's activities, including the Licensee's use of third-party service providers, and the sensitivity of the nonpublic information used, possessed, or controlled by the Licensee.

Implement Safeguards to Protect Nonpublic Information

The Security Program must contain administrative, technical, and physical safeguards to protect nonpublic information and shall:

- Protect the security and confidentiality of the nonpublic information and the security of the information system;
- Protect against any threats or hazards to the security or integrity of the nonpublic information and the information system;
- Protect against unauthorized access to or use of the nonpublic information and minimize the likelihood of harm to any consumer; and
- Define and periodically reevaluate a schedule for retention of the nonpublic information, along with a mechanism for its destruction when no longer needed.

Conduct Risk Assessments

Each Licensee must conduct risk assessments that:

- Identify reasonably foreseeable internal or external threats that could result in unauthorized access or destruction of nonpublic information, including threats to the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers;
- Assess the likelihood and potential damage of internal and external threats, taking into consideration the sensitivity of the nonpublic information;
- Assess the sufficiency of the policies, procedures, information systems, and other safeguards in place to manage the internal and external threats, including: (i) Employee training and management, (ii) Information systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal, and (iii) Detecting, preventing, and responding to attacks, intrusions, or other system failures;
- Implement information safeguards to manage the threats identified in its ongoing assessment; and
- Asses the effectiveness of the safeguards' key controls, systems, and procedures, not less than annually.

Address Certain Security Vulnerabilities

The Licensee must use the outcomes from its internal risk assessment to undertake the following:

- Determine which, if any, of the following security measures are appropriate and implement such security measures:
  - Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals, to protect against the unauthorized acquisition of nonpublic

information;

- Identify and maintain the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;
- Restrict access to physical locations containing nonpublic information;
- Protect by encryption or other appropriate means all nonpublic information while such information is being transmitted over an external network and all nonpublic information stored on a laptop or other portable computing or storage device or media;
- Adopt secure development practices for in-house developed applications and procedures for evaluating, assessing, or testing the security of externally developed applications;
- Modify the information system in accordance with the Security Program;
- Utilize effective controls, which may include multifactor authentication procedures for accessing nonpublic information;
- Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusion into, information systems;
- Include audit trails within the information security program designed to detect and respond to cybersecurity events and reconstruct material financial transactions sufficient to support normal operations and obligations of the Licensee;
- Implement measures to protect against destruction, loss or damage of nonpublic information due to environmental hazards; and
- Implement procedures for the secure disposal of nonpublic information.

- Include cybersecurity risks in the Licensee's enterprise risk management process;
- Stay updated on emerging threats or vulnerabilities and utilize reasonable security measures when sharing information; and
- Provide personnel with cybersecurity awareness training that reflects the risks identified by the Licensee in its risk assessment process.

Designate Responsibility for Data Security – Starting with the Board of Directors

The Licensee's Board of Directors, or a committee thereof, must:

- Require executive management to develop, implement and maintain the Security Program; and
- Require executive management to report annually to the Board of Directors the overall status of the Security Program, compliance with the cybersecurity requirements, and any material matters related to the Security Program, including risk assessment, management and controls, third-party service provider arrangements, results of testing, cybersecurity events and management's response, and recommendations regarding changes to the Security Program.

Additionally, one or more persons or entities must also be designated to act on behalf of the Licensee and be responsible for the Security Program.

Increase Diligence over Third Party Providers

Within two years of the Effective Date, Licensees are also required to exercise due diligence surrounding the selection of its various third-party providers that maintain, process, or store nonpublic information or that otherwise have access to the Licensee's nonpublic information in connection with the services they provide. Licensees are mandated to require their third-party service providers to implement appropriate administrative, technical and physical measures and safeguards to protect and secure the nonpublic information that is accessible to, or held by, the third-party service provider.

Implement Written Incident Response Plan

Licensees are required to establish and maintain a written incident response plan that is designed to respond to and recover from any cybersecurity event. The Incident Response Plan must address at least the following:

- Internal processes for responding to a cybersecurity event;
- Goals of the Incident Response Plan;
- Definition of clear roles, responsibilities, and levels of decision-making authority;
- External and internal communications and information sharing;
- Requirements for the remediation of any identified weaknesses in Licensee's information systems and associated controls;
- Documentation and reporting of cybersecurity events and related incident response activities; and
- Evaluation and revision as necessary of the Incident Response Plan following a cybersecurity event.

Report Cybersecurity Events to the Ohio Department of Insurance

If a Licensee learns that a cybersecurity event has or may have occurred, the Licensee is required to conduct a prompt investigation to determine whether the cybersecurity event did in fact occur. The investigation must assess the nature and scope of the cybersecurity event, identify any nonpublic information that may have been disclosed, and perform reasonable measures to secure the information systems compromised in the cybersecurity event.

The Superintendent of Insurance must be notified as promptly as possible once the Licensee has confirmed a cybersecurity event involving nonpublic information occurred. However, this prompt notification must be completed within three (3) business days if the Licensee meets certain codified criteria. The notice must contain as much information as possible about the cybersecurity event and must be updated with material developments as the investigation proceeds.

Licensees must maintain records concerning cybersecurity events for at least five (5) years from the date of the event.

Importantly, not every cybersecurity event is reportable under the law. The definition of a "cybersecurity event" excludes instances where the compromised information was encrypted and the encryption, process, or key is not also compromised. The definition also excludes instances where the Licensee's

investigation determines that the nonpublic information accessed by an unauthorized person has not been used or released and the nonpublic information was returned or destroyed.

Certify Compliance Each Year

Each insurance company domiciled in Ohio, except for an insurance company that is domiciled in Ohio and exclusively licensed in Ohio, shall submit annually, on or before February 15, a written statement certifying that it is in compliance with the Ohio Cybersecurity Law. An insurance company that is licensed exclusively in Ohio is permitted to include this annual certification as part of its Corporate Governance Annual Disclosure filing due June 1 under Section 3901.073 of the Ohio Revised Code.

Other Key Provisions

In addition to these requirements, the Ohio Cybersecurity Law contains several key provisions to assist with compliance. For example, Licensees who are covered by the Security Program of another licensee do not have to develop a separate Security Program of their own. In the event a Licensee no longer qualifies for one of the law's exemptions, the Licensee will have one hundred eighty (180) days after the date it ceases to qualify for the exemption to comply with the cybersecurity requirements.

Licensees who comply with Ohio Cybersecurity Law may also qualify under Ohio's Data Protection Act for an affirmative defense to certain tort actions. More information about Ohio's Data Protection Act is available here. Additionally, materials furnished to the Superintendent in connection with compliance with the Ohio Cybersecurity Law are considered confidential, privileged, not considered a public record, not subject to subpoena and shall not be subject to discovery or admissible as evidence in any private civil action. However, the Superintendent may use these documents and other information for regulatory or legal action brought as part of the Superintendent's duties.

Next Steps

Licensees should have their IT, legal, and corporate governance teams collaborate to develop a tailored approach to comply with these new robust requirements. A generic, one-size-fits-all approach will not work. In addition, directors of Licensees should be promptly advised of the resources and responsibilities that will be necessary to achieve timely compliance. It should also be understood that the process is organic and will continue to evolve as Licensees' business and technology change.

This summary is qualified in its entirety by the Ohio Cybersecurity Law and ORC Chapter 3965. For more information or questions regarding the Ohio Cybersecurity Law and ORC Chapter 3965, or developing a program to comply with this new law, please contact Anthony Spina, Tom Szykowny, John Landolfi, Chris Ingram, or your Vorys attorney.