THOMPSON HINE

Privacy & Cybersecurity Update

March 2024

Florida and West Virginia Create New Cybersecurity Safe Harbor Laws

Cybersecurity events, such as ransomware attacks and business email compromises, can impact even the best-prepared business. Unfortunately, a corporate victim of a cybersecurity event may itself become the target of litigation or government enforcement actions, adding costly insult to serious injury. Recently, the Florida and West Virginia Legislatures crafted legislation seeking to provide companies with certain limited protection from private litigation after they suffer a data breach despite their cybersecurity planning and execution. Once these legal frameworks are enacted into law, businesses subject to them will be able to undertake certain measures to invoke cybersecurity safe harbor provisions to obtain legal liability protection if they suffer a data breach.

Florida HB 473

Recently, the Florida Legislature passed House Bill 473, which will enter into force if (or, more likely, "when") signed into law by Governor Ron DeSantis. HB 473 provides certain liability protection for state governments and commercial entities (and their agents). Specifically, it provides that private-sector organizations that maintain personal information will not be "liable in connection with a cybersecurity incident" if they substantially comply with Florida's personal data breach notification statute *and* have adopted a cybersecurity program that substantially aligns with certain standards, guidelines, or regulations, which include (but are not limited to) the following:

- The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, NIST special publication 800-171, or NIST special publications 800-53 and 800-53A
- The Federal Risk and Authorization Management Program security assessment framework
- The Center for Internet Security (CIS) Critical Security Controls
- The International Organization for Standardization/ International Electrotechnical Commission 27000 series (ISO/IEC 27000) family of standards
- HITRUST Common Security Framework (CSF)
- Service Organization Control Type 2 (SOC 2) Framework
- Secure Controls Framework
- Other similar industry frameworks or standards

Entities regulated by state or federal cybersecurity standards (e.g., healthcare entities, financial institutions) would be required to comply with these applicable standards for the liability protections to apply.

HB 473 also provides that an organization can demonstrate "substantial alignment" with these cybersecurity frameworks "by providing documentation or other evidence of an assessment, conducted internally or by a third party, reflecting that [its] cybersecurity program is substantially aligned with the relevant framework or standard or with the applicable state or federal law or regulation." Such an assessment must take into account the size and complexity of the covered entity, the nature and scope of its activities, and the sensitivity of the information to be protected. These organizations must, within one year, update their cybersecurity program to "substantially align" with any amendments made to cybersecurity frameworks approved within the law.

In an action relating to a cybersecurity incident, the defendant (i.e., the covered entity) has the burden of proof to establish substantial compliance.

Importantly, the law does not define "cybersecurity incident" or "personal information," nor does it seek to describe the scope of the law's immunity. These issues will likely be resolved by the courts.

West Virginia HB 5338

As noted above, West Virginia also recently adopted a cybersecurity safe harbor statute, House Bill 5338, although it contains more detail than other similar state laws and appears to be narrower than Florida HB 473.

HB 5338 provides that a covered entity that creates, maintains, and complies with certain cybersecurity standards is "entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information."

A covered entity is defined as "a business that accesses, maintains, communicates, or processes *personal information* or *restricted information* in or through one or more systems, networks, or services located in or outside this state." The terms "personal information" and "restricted information" relate to various types of personally identifiable information with varying degrees of sensitivity.

HB 5338 provides that a cybersecurity program must contain administrative, technical, operational, and physical safeguards, and shall be designed to do all of the following:

- Continually evaluate and mitigate any reasonably anticipated internal or external threats or hazards that could lead to a data breach
- Periodically evaluate no less than annually the maximum probable loss attainable from a data breach
- Communicate to any affected parties the extent of any risk posed and any actions the affected parties could take to reduce any damages if a data breach is known to have occurred

HB 5338 also provides that the "scale and scope" of a cybersecurity program is "appropriate" if its operational costs are "no less than the covered entity's most recently calculated maximum probable loss value."

A covered entity satisfies all the of the law's requirements if its cybersecurity program "reasonably conforms" to any of the following cybersecurity programs:

- The NIST Framework for Improving Critical Infrastructure Cybersecurity, NIST special publication 800-171, or NIST special publications 800-53 and 800-53A
- The Federal Risk and Authorization Management Program security assessment framework
- The CIS Critical Security Controls
- The ISO/IEC 27000 family of standards
- The Cybersecurity Maturity Model Certification at a minimum of Level 2 with external certification

Entities regulated by state or federal cybersecurity standards (e.g., healthcare entities, financial institutions) would be required to comply with these applicable standards for the liability protections to apply.

When any revisions to these frameworks are published, a covered entity must adopt them "within the time frame provided in the relevant framework upon which the covered entity intends to rely to support its affirmative defense, but in no event later than one year after the publication date stated in the revision."

HB 5338 separately addresses educational institutions' cybersecurity programs, providing that "[a]ny institution of higher education in [West Virginia] may offer a cybersecurity assessment program as part of an undergraduate or graduate program relating to cybersecurity to any business in the state." It further provides that such an institution, *or* any employee or student thereof, offering these cybersecurity assessment programs are "immune from civil liability that arises from the failure of a covered entity to conform to the provisions of this article."

Next Steps: Strategy Development

To effectively and efficiently avail themselves of these cybersecurity safe harbor statutes, businesses should consider the following three areas.

Formalize existing security measures. Many businesses have already implemented some technical, physical, and administrative data security measures to protect data in their custody and control. For example, businesses routinely

use encryption protocols, firewalls, and other technical programs to safeguard corporate data, as well as incident response procedures, confidentiality requirements, and other administrative security measures. However, these safeguards, plans, and policies may have been generated and implemented in a disparate and inconsistent manner. To identify the scope of cybersecurity programs and demonstrate compliance with cybersecurity standards set forth in the safe harbor laws, these policies should be reviewed and consolidated under a unified, *written* cybersecurity plan.

Identify where the program aligns. Once a business determines the scope of its existing cybersecurity program, it should compare and contrast it to the acceptable frameworks set forth in the cybersecurity safe harbor laws to identify the security framework with which it most closely aligns. Thereafter, the business will be better positioned to more narrowly create and implement the remaining elements of the cybersecurity framework needed to satisfy the safe harbor provision.

Satisfy outstanding requirements. Once a business determines the acceptable cybersecurity framework with which it most closely aligns, it should implement any outstanding physical, technical, and administrative measures needed to satisfy the framework's remaining requirements. In addition, to ensure that a business can rely upon the safe harbor provision, it will need to establish an internal or external process to continuously monitor its cybersecurity program for compliance purposes.

Conclusion

The new laws in Florida and West Virginia and similar laws in other states (e.g., Connecticut, Ohio, Utah) provide incentives for companies to adopt cybersecurity measures to protect personal information in their custody and control. Cyberattacks continue to increase in scope and sophistication, and these statutes offer a valuable safe harbor to businesses that proactively build a cybersecurity program.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com