OHIO LEGISLATIVE SERVICE COMMISSION

Bill Analysis

Cody Weisbrodt

Sub. S.B. 220*

132nd General Assembly
(As Reported by H. Government Accountability & Oversight)

Sens. Hackett and Bacon, Burke, Dolan, Hoagland

BILL SUMMARY

Cybersecurity program affirmative defense

- Creates an affirmative defense to a tort action against a covered entity because of a data breach, if the entity is accused of failing to implement reasonable information security controls and the entity has a cybersecurity program that meets the bill's requirements.

Definitions

- Defines "covered entity" as a business or nonprofit entity, including a financial institution, that accesses, maintains, communicates, or handles personal information or restricted information.

- Provides definitions for "personal information," "restricted information," and "data breach."

Requirements to qualify for the affirmative defense

- Requires a covered entity, in order to be eligible for the affirmative defense, to create, maintain, and comply with a written cybersecurity program that contains certain safeguards for the protection of personal information, restricted information, or both.

* This analysis was prepared before the report of the House Government Accountability & Oversight Committee appeared in the House Journal. Note that the list of co-sponsors and the legislative history may be incomplete.

- Requires the cybersecurity program to meet the bill's design, scale, and scope requirements and to reasonably conform to an industry recognized cybersecurity framework listed in the bill.

- Allows a covered entity to have a cybersecurity program that protects personal information and therefore to be entitled to an affirmative defense to a cause of action involving a data breach concerning personal information.

- Allows a covered entity instead to have a cybersecurity program that protects both personal information and restricted information and therefore to be entitled to an affirmative defense to a cause of action involving a data breach concerning personal information or restricted information.

Other provisions

- Specifies that the bill does not provide a private right of action that would allow a person to sue a covered entity for failing to follow the bill's cybersecurity requirements.

- Specifies that the bill's provisions are severable.

- States that the bill is intended to encourage improved cybersecurity through voluntary action and not to create a minimum cybersecurity standard that must be achieved.

Blockchain transactions permitted

- Specifies that transactions recorded by blockchain technology are permitted under the Uniform Electronic Transactions Act.

Key employee definition in the Casino Law

- Reorganizes the definition of key employee in the Casino Law to remove repetitive language.

- Raises the threshold of direct or indirect ownership in a person that applies for or holds a casino operator, management company, or gaming-related vendor license that requires an individual to obtain a key employee license from one percent to five percent.

- Eliminates the ability of the Ohio Casino Control Commission to determine whether an individual whose duties differ from those included in the definition of "key employee" should be considered a key employee.

CONTENT AND OPERATION

Cybersecurity program affirmative defense

The bill creates an affirmative defense to any tort action against a covered entity because of a data breach, if the entity is accused of failing to implement reasonable information security controls to prevent the breach. To be eligible to use the affirmative defense, the entity must have a cybersecurity program that meets the bill's requirements. The bill refers to the affirmative defense as a "safe harbor."

(A tort action is a civil lawsuit for a legal wrong or injury, such as negligence, for which the person bringing the lawsuit seeks compensation for damages. An affirmative defense is a factor that, if proven by the defendant, makes the defendant not liable for the damages.)

Definitions

Covered entities

Under the bill, a "covered entity" is a business that accesses, maintains, communicates, or handles personal information or restricted information in or through one or more systems, networks, or services located in or outside Ohio. "Business" means any limited liability company (LLC), limited liability partnership (LLP), corporation, sole proprietorship, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of Ohio, any other state, the United States, or any other country, or the parent or subsidiary of any of the foregoing.[1]

Personal information

The bill specifies that "personal information" has the same meaning as in Ohio's Consumer Protection Law. Under that law, personal information means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology to make them unreadable:

- The individual's Social Security number;
- The individual's driver's license or state identification card number;

[1] R.C. 1354.01(A) and (B).

- The individual's account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to the individual's financial account.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed:

- Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television;

- Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to those news media;

- Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation;

- Any type of media similar in nature to any of those items, entities, or activities.[2]

Restricted information

Under the bill, "restricted information" means any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual, if the information is not encrypted, redacted, or altered by any method or technology to make it unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property. ("Encrypted," "individual," and "redacted" have the same meanings as in the Consumer Protection Law.)[3]

For example, if an unencrypted database contained only an individual's residence address, birthdate, and driver's license number, that information would not be considered personal information under the bill because it did not include the person's name, but it could be considered restricted information it would be possible to identify the person based on the information, and a court could determine that the breach of that data would likely constitute a material risk of identity theft or fraud.

[2] R.C. 1354.01(D). See also R.C. 1349.19(A)(7), not in the bill.

[3] R.C. 1354.01(E).

Data breach

Under the bill, "data breach" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information or restricted information owned by or licensed to a covered entity and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to person or property.

For purposes of that definition, good faith acquisition of personal information or restricted information by an employee or agent of the covered entity for purposes of the covered entity is not a data breach, provided that the information is not used for an unlawful purpose or subject to further unauthorized disclosure. And, acquisition of personal information or restricted information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a data breach.[4]

Requirements to qualify for the affirmative defense

To be eligible to use the bill's affirmative defense, a covered entity must do one of the following:

(1) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of *personal information*, that meets the bill's design, scale, and scope requirements, and that reasonably conforms to an industry recognized cybersecurity framework listed in the bill; or

(2) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of *both personal information and restricted information*, that meets the bill's design, scale, and scope requirements, and that reasonably conforms to an industry recognized cybersecurity framework listed in the bill.

A covered entity that satisfies the requirements under (1) above is entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of Ohio or in the courts of Ohio and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information. A covered entity that satisfies the requirements under (2) above is entitled

[4] R.C. 1354.01(C).

to an affirmative defense to any such cause of action involving a data breach concerning personal information or restricted information.[5]

Cybersecurity program requirements

The bill requires a covered entity's cybersecurity program to be designed to do all of the following with respect to the information it is meant to protect:[6]

- Protect the security and confidentiality of the information;
- Protect against any anticipated threats or hazards to the security or integrity of the information;
- Protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

The scale and scope of a covered entity's cybersecurity program is considered appropriate if it is based on all of the following factors:[7]

- The entity's size and complexity of the covered entity;
- The nature and scope of the entity's activities;
- The sensitivity of the information to be protected;
- The cost and availability of tools to improve information security and reduce vulnerabilities;
- The resources available to the covered entity.

Approved cybersecurity frameworks

Under the bill, a covered entity's cybersecurity program also must reasonably conform to an industry recognized cybersecurity framework. The program meets that requirement if one of the following apply:[8]

---

[5] R.C. 1354.02(A) and (D).

[6] R.C. 1354.02(B).

[7] R.C. 1354.02(C).

[8] R.C. 1354.01(E) and 1354.03(A).

- The program reasonably conforms to the current version of any of the following or any combination of the following frameworks:

    - The Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology (NIST);

    - NIST Special Publication 800-171;

    - NIST Special Publications 800-53 and 800-53a;

    - The Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework;

    - The Center for Internet Security Critical Security Controls for Effective Cyber Defense;

    - The International Organization for Standardization/International Electrotechnical Commission 27000 Family – Information Security Management Systems.

- The program reasonably complies with the current version of the Payment Card Industry (PCI) Data Security Standard and conforms to the current version of another applicable framework listed above.

- The covered entity is regulated by the state, by the federal government, or both, or is otherwise subject to the requirements of any of the laws or regulations listed below, and the program reasonably conforms to the entirety of the current version of any of the following:[9]

    - The security requirements of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), which governs healthcare;

    - Title V of the federal Gramm-Leach-Bliley Act of 1999, which applies to financial institutions;

    - The Federal Information Security Modernization Act of 2014, which generally covers federal agencies;

[9] R.C. 1354.03(B).

- The Health Information Technology for Economic and Clinical Health Act, which applies to healthcare providers.

When a final revision to a cybersecurity framework in the first list above is published, a covered entity whose cybersecurity program reasonably conforms to that framework must reasonably conform to the revised framework not later than one year after the publication date stated in the revision. And, when a statutory framework in the second list above is amended, a covered entity whose cybersecurity program reasonably conforms to that framework must reasonably conforms to the amended framework not later than one year after the effective date of the amended framework.

Finally, if a covered entity's cybersecurity program reasonably conforms to a combination of industry recognized cybersecurity frameworks, other than the statutory frameworks in the second list above, (or complies with a standard, as in the case of the PCI Data Security Standard) and two or more of those frameworks are revised, the entity must as applicable reasonably conform to, or comply with, all of the revised frameworks not later than one year after the latest publication date stated in the revisions.[10]

Other provisions

No private right of action

The bill specifies that it does not provide a private right of action, including a class action, with respect to any act or practice regulated under the bill. In other words, the bill does not allow a person to sue a covered entity for failing to follow the bill's cybersecurity requirements, unless another law would allow the person to do so.[11]

Severability

The bill specifies that if any of its provisions or the application of those provisions to a covered entity is ruled invalid, the remainder of those provisions and their application to other entities is not affected. (The Revised Code provides generally that this principle of severability applies to all Ohio statutes.)[12]

Legislative intent

The bill states that its purpose is to establish a legal safe harbor to be pled as an affirmative defense, as described above. It also states that the bill is intended to be an

[10] R.C. 1354.02(D).

[11] R.C. 1354.04.

[12] R.C. 1354.05. See also R.C. 1.50, not in the bill.

incentive and to encourage businesses to achieve a higher level of cybersecurity through voluntary action. It does not, and is not intended to, create a minimum cybersecurity standard that must be achieved, nor may it be read to impose liability upon businesses that do not obtain or maintain practices in compliance with the bill.[13]

Blockchain transactions permitted

The bill states that a record or contract secured through blockchain technology is considered to be in an electronic form and to be an electronic record, and that a signature secured through blockchain technology is considered to be in an electronic form and to be an electronic signature for the purposes of Ohio's Uniform Electronic Transactions Act.[14]

Definition of key employee in the Casino Law

The bill reorganizes the definition of "key employee" under the Casino Law to remove repetitive language.[15] In the bill, "key employee" means any executive, employee, agent, or other individual who has the power to exercise significant influence over decisions concerning any part of the operation of a person that has applied for or holds a casino operator, management company, or gaming-related vendor license or gaming-related vendor license, or the operation of a holding company of a person that has applied for or holds a casino operator, management company, or gaming-related vendor license, including:

(1) An officer, director, partner, or equivalent fiduciary;

(2) An individual who holds a direct or indirect ownership interest of five percent or more;

(3) An individual who performs the function of a principal executive officer, principal operating officer, principal accounting officer, or an equivalent officer;

(4) Any other individual the Ohio Casino Control Commission determines to have the power to exercise significant influence over decisions concerning any part of the operation.

The bill raises the threshold of direct or indirect ownership that requires an individual to obtain a key employee license from one percent in current law to five

[13] Section 2 of the bill.

[14] R.C. 1306.01.

[15] R.C. 3772.01(P).

percent, and also removes a provision in current law that allows the Commission to determine whether an individual whose duties or status varies from those described is considered a key employee.

HISTORY

ACTION	DATE
Introduced	10-17-17
Reported, S. Gov't Oversight & Reform	05-16-18
Passed Senate (24-8)	05-16-18
Reported, H. Gov't Accountability & Oversight	---

S0220-RH-132.docx/ec