LOCKE LORD® QUICK Study
Privacy & Cybersecurity Practice
November 26, 2018

New Data Security Law Offers Safe Harbor; May Signal New Trend

By: Tom Smedinghoff, Dave Szabo and Brandan Montminy

A first-of-its-kind data security law, the recently enacted Ohio Data Protection Act[1] may signal the beginning of a new trend in the legal approach to corporate cybersecurity obligations. At the same time, it may provide some assistance to businesses struggling to ensure that they have implemented legally required data security.

Titled "An Act...to provide a legal safe harbor to covered entities that implement a specified cybersecurity program..." the Ohio Data Protection Act took effect on November 1, 2018 and introduces two very important concepts relevant to cybersecurity compliance.

- First, the Act implicitly recognizes that compliance with selected industry norms and best practices provides legally compliant "reasonable security;" and
- Second, for businesses that follow one of the approaches designated in the Act, the Act provides a safe harbor in the form of an affirmative defense to any tort action that is brought against the business alleging that its failure to implement reasonable information security controls resulted in a data breach concerning personal information.

The Act applies to any business that accesses, maintains, communicates, or processes "personal information" and/or "restricted information." Those terms are defined as follows:

- "Personal information" covers an individual's name (consisting of the individual's first name or first initial and last name), in combination with any one of the following: (i) Social security number; (ii) Driver's license number or state identification card number; (iii) 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 an individual's financial account.[2]
- "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 in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property.

To obtain the benefit of the affirmative defense, a business must "create, maintain, and comply with a written cybersecurity program" that satisfies three requirements. The cybersecurity program must:

- "Contain administrative, technical, and physical safeguards for the protection of personal information [or personal information and restricted information] *that reasonably conforms to an industry recognized cybersecurity framework* as described in [the Act]."[3]
- "Be designed to do all of the following with respect to the [personal and/or restricted information]," as applicable:
    i. Protect the security and confidentiality of the information;
    ii. Protect against any anticipated threats or hazards to the security or integrity of the information;

1 ORC 1354 et seq.
2 ORC 1354.01(D); 1349.19.
3 ORC 1354.02(A) (emphasis added)

iii. 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, and[4]

- Be appropriate in "scale and scope" based on all of the following factors:
  i. The size and complexity of the covered entity;
  ii. The nature and scope of the activities of the covered entity;
  iii. The sensitivity of the information to be protected;
  iv. The cost and availability of tools to improve in formation security and reduce vulnerabilities;
  v. The resources available to the covered entity.[5]

Businesses that meet these requirements are entitled to an affirmative defense to any cause of action sounding in tort brought under the laws of Ohio or in the courts of Ohio alleging that the failure to implement reasonable information security controls resulted in a data breach concerning personal information, or restricted information.[6]

The "industry-recognized cybersecurity frameworks" that qualify for the safe harbor under the Act (and to which an organization's cybersecurity program must "reasonably conform") are the following –

For all businesses:

- NIST Cybersecurity Framework[7]
- NIST Special Publication 800-171 ("Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations")[8]
- NIST Special Publications 800-53[9] ("Security and Privacy Controls for Information Systems and Organizations") and 800-53A ("Assessing Security and Privacy Controls in Federal Information Systems and Organization")[10]
- The Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework[11]
- Center for Internet Security, Critical Security Controls for Effective Cyber Defense[12]
- International Organization for Standardization / International Electrotechnical Commission 27000 Family of Information Security Standards - information security management systems ISO-27000 family[13]

For regulated businesses:

- HIPAA security requirements
- GLB security requirements
- FISMA
- Health Information Technology for Economic and Clinical Health Act
- PCI standard

This approach appears to recognize that cybersecurity programs based on any of the foregoing provide "reasonable security," and that providing "reasonable security" is a defense in the case of a breach.

---

4 ORC 1354.02(B)
5 ORC 1354.02(C)
6 ORC 1354.02(D)
7 NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (April 16, 2018); available here.
8 NIST SP 800-171, Rev. 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (December 2016); available here.
9 NIST SP 800-53, Rev 5, "Security and Privacy Controls for Information Systems and Organizations,(August 2017); available here.
10 NIST SP 800-53A, Rev 4, Assessing Security and Privacy Controls in Federal Information Systems and Organization (December 18, 2014); available here.
11 FedRAMP Security Assessment Framework, Ver. 2.4 (November 15, 2017); available here.
12 CIS Controls, available here.
13 ISO/IEC 27000 Family of Information Security Standards

This Ohio statute is the first cybersecurity law providing an express safe harbor for entities that exercise "reasonable security". However, it should be noted that a few years ago the California Attorney General released a report setting forth what might be described as a reverse safe harbor – i.e., if you don't take certain steps, then you will be deemed *not* to have provided legally compliant reasonable security.

In the "California Data Breach Report 2012 – 2015,"[14] the California Attorney General referenced the requirement under California law that businesses implement "reasonable" security,[15] and noted that the Center for Internet Security's Critical Security Controls for Effective Cyber Defense (the Controls)[16] are designed to address this challenge.[17] But then the Report went further, stating that failure to implement those Controls constitutes a lack of reasonable security. Specifically, the Report states that:

> The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. *The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.*[18]

It is unclear whether either the safe harbor approach adopted by the Ohio statute or the so-called reverse safe harbor approach promoted by the California Attorney General will gain traction. But as businesses struggle with the issue of defining "reasonable security," we can probably expect to see more law and regulation along these lines.

For more information on the matters discussed in this *Locke Lord QuickStudy*, please contact the authors.

Tom Smedinghoff | 312-201-2021 | tom.smedinghoff@lockelord.com
Dave Szabo | 617-239-0414 | david.szabo@lockelord.com
Brandan Montminy | 214-740-8445 | brandan.montminy@lockelord.com

14 California Data Breach Report 2016, California Attorney General (February 2016), at p. 27-34.
15 See Cal. Civ. Code § 1798.81.5(b), "A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."
16 The CIS Critical Security Controls for Effective Cyber Defense, Version 6, October 15, 2015, available from the Center for Internet Security. Formerly known as the SANS Top 20, the Controls are now managed by the Center for Internet Security (CIS), a non-profit organization that promotes cybersecurity readiness and response by identifying, developing, and validating best practices.
17 Id, at p. 30.
18 Id. (emphasis added)