Armstrong Teasdale

February 15, 2021 • Advisory • www.atllp.com

OUTLIER OR PIONEER? UTAH RECONSIDERS A CYBERSECURITY "SAFE HARBOR"

Last year the Utah legislature was poised to consider the Cybersecurity Affirmative Defense Act (the Proposed Act). Then in one fell swoop, the Proposed Act was sidelined by a pandemic that nationally announced itself in March 2020.

Now, like last year's act, the Proposed Act, which would provide a safe harbor for organizations that implement specific cybersecurity standards, is back. Put another way, if at the time of a "breach of system security" an organization has created, maintained and complied with a written cybersecurity program, it would have an affirmative defense to a civil tort claim such as negligence.

Under the Proposed Act, a "breach of system security" would mean unauthorized acquisition of computerized data maintained by a person or organization that compromises the security, confidentiality or integrity of personal information. The Proposed Act would require that a covered entity's written cybersecurity program be designed to:

1. protect the security and confidentiality of personal information;
2. protect against any anticipated threat or hazard to the security or integrity of personal information; and
3. protect against a breach of system security.

The Proposed Act would also require that a covered entity's written cybersecurity program "reasonably conform to an industry recognized cybersecurity framework." It lists "the framework for improving critical infrastructure developed by [the National Institute of Standards and Technology]" (NIST) and the "Center for Internet Security Critical Controls for Effective Cyber Defense" (CIS), among others, as industry recognized.

Just as Utah's digital transformation has been a few years in the making, the Proposed Act is not Utah's first cybersecurity rodeo. Utah is the first state to enact the Electronic Information or Data Privacy Act which prohibits law enforcement from obtaining personal electronic information from third parties without a warrant,[1] and the second state to enact the Computer Abuse and Data Recovery Act, which prohibits the unauthorized use and/or access of

PEOPLE
Casey E. Waughn, CIPP/US

SERVICES AND INDUSTRIES
Data Innovation, Security and Privacy

computers, platforms or data.[2] The Proposed Act is also not the first of its kind.

Cybersecurity Safe Harbors - An Incentive for Organizations to Safeguard Personal Information

In 2018, the Ohio legislature enacted the Ohio Data Protection Act. Just like the Proposed Act, the Ohio Act enables a defendant in lawsuits to assert as an affirmative defense that it safeguards personal information or has a written cybersecurity program that conforms to an industry-recognized cybersecurity framework.[3] The Ohio Act does not use the term "breach of system security" but instead uses the term "data breach" which means something substantially similar.[4]

Under the Ohio Act, just like the Proposed Act, an "industry-recognized cybersecurity framework" is limited to frameworks promulgated by certain industry organizations (e.g., NIST, CIS and the Payment Card Industry Data Security Standard (PCI)) and applicable regulatory schemes (e.g., the Health Insurance Portability and Accountability Act (HIPAA) for protected health information, and the Gramm-Leach-Bliley Act (GLBA) for financial institutions).

New York has a similar but narrower version of the Proposed Act and the Ohio Act. Enacted in 2020, New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) requires that organizations that collect data maintain reasonable security[5] according to applicable regulatory schemes (e.g., GLBA, HIPAA) and also specific agencies such as the New York State Education Department and its Department of Motor Vehicles. Just as the Proposed Act is not the first to provide a cybersecurity safe harbor, it is also not the first to require a written cybersecurity program.

Written Information Security Programs (WISPs) – An Industry Standard

Oregon,[6] Massachusetts[7] and Rhode Island[8] require organizations to develop and implement a WISP that includes administrative, technical and physical safeguards for personal information. Each of these states provides detailed requirements of what should be included. Key elements include:

- proper training for employees about appropriate cybersecurity best practices;
- auditing programs and practices regularly to ensure they are reasonable and appropriate considering the data collected and resources of the organization;
- designating an employee to oversee the WISP; and
- maintaining an incident response plan that details how an organization will respond to a breach of system security or data breach.

A WISP should also include a section that addresses how an organization will ensure its vendors safeguard personal information. Indeed, last month the Federal Trade Commission (FTC) entered into a settlement with a mortgage

analytics company that the FTC alleged failed to vet a vendor that provided text recognition services for mortgage documents. That vendor had inadvertently exposed the personal information of tens of thousands of consumers from January 2018–January 2019. In the settlement, the mortgage company must establish a vendor management program.

Oregon, Massachusetts and Rhode Island[9] all require organizations to not only select vendors capable of implementing appropriate security practices, but to maintain contracts with these vendors regarding security safeguards and practices. It naturally follows then, that the Proposed Act will also require organizations to ensure that vendors have administrative, technical and physical safeguards in place for any personal information that organizations provide to their vendors.

Just as cybersecurity threats continue to rapidly evolve, so too does the legal landscape and industry standards designed to safeguard personal information. If you have any questions about the Proposed Act, the safe harbors provided in other similar statutes, or would like to consult about your organization's WISP, please contact your regular AT attorney or one of those listed on this advisory.

[1] Utah Code. Ann. § 77-23c-102.

[2] Utah Code. Ann. § 63D-3-10.

[3] Ohio Rev. Code Ann. § 1354.02.

[4] Ohio Rev. Code § 1354.01.

[5] N.Y. Gen. Bus. Law § 899-bb.

[6] Or. Rev. Stat § 646A.622.

[7] 201 Mass. Code Regs. 17.03.

[8] R.I. Gen. Laws § 11-49.3-2.

[9] Or. Rev. Stat § 646A.622(2)(d); 201 Mass. Code Regs. 17.03(2)(f); R.I. Gen. Laws § 11-49.3-2(b).