# UTAH'S CYBERSECURITY AFFIRMATIVE DEFENSE ACT PROVIDES AN INCENTIVE TO IMPLEMENT A CYBERSECURITY PROGRAM

BY ELAINA M. MARAGAKIS

If you needed a(nother) reason to implement a cybersecurity program, the 2021 general session of the Utah Legislature has answered the call.[1]

The Utah Cybersecurity Affirmative Defense Act ("Act") HB80, effective May 1, 2021, ushered in bold change for the way in which a "person,"[2] addresses cybersecurity. In brief, the Act provides an entity with an affirmative defense to specific claims in state litigation if the entity has created, maintained, and reasonably complied with a written cybersecurity program that satisfies certain criteria.

The Act represents a sea change in mechanisms designed to compel compliance with cybersecurity laws. Rather than punishing an entity *after* a data breach for failing to have adequate security measures in place, the Act encourages action *before* a data breach occurs by providing an incentive—as Representative Walt Brooks (who sponsored the Act) put it, a "carrot"—for an entity to shore up security on the front end. This preventive approach is designed to motivate an entity to overhaul its security practices. The legislature's hope is that "the . . . industry [as] a whole will raise their standards because now there is a benefit" to being proactive.[3]

The Act provides, "[a] person that creates, maintains, and reasonably complies with a written cybersecurity program that meets [specific] requirements, and is in place at the time of a breach of system security of the person, has an affirmative defense to a claim that: (a) is brought under the laws of this state or in the courts of this state; and (b) alleges that a person failed to implement reasonable information security controls that resulted in the breach of system security." Utah Code Ann. § 78B-4-702.

Notably, the cybersecurity program must be *written*. It is not enough to have vague cybersecurity protocols that are simply expressed verbally, or implemented only in practice. Instead, an entity must take a more formal, extensive review of the flow of information on an enterprise-wide level, and carefully craft custom written policies that address its specific industry. Thus, the Act gives a much needed boost to cybersecurity efforts which may have languished because of other, more pressing, initiatives.

The Act also breaks new ground in Utah by setting forth very specific standards by which to measure the adequacy of an entity's policies and procedures.

Under the Act, a cybersecurity program must provide administrative, technical, and physical safeguards to protect personal information, including:

- being designed to:
    - o protect the security, confidentiality, and integrity of personal information;
    - o protect against any anticipated threat or hazard to the security, confidentiality, or integrity of personal information; and
    - o protect against a breach of system security
- Reasonably conform to a recognized cybersecurity framework; and
- Be of an appropriate scale and scope in light of enumerated factors.

Utah Code Ann. § 78B-4-702(4).

While businesses have long struggled to implement programs using largely undefined standards and vague language such as "administrative, technical, and physical safeguards," the Act helpfully addresses the issue of what constitutes reasonable conformity with a "recognized cybersecurity framework" by offering a range of specific options, including a list—by name—of published, readily available publications from which an entity can draw. *Id.* §§ 78B-4-702(4); 78B-4-703(1). Specifically, a qualifying cybersecurity program must be designed to protect the type of personal information obtained in the breach of system security, and must:

i. conform with a "reasonable security program" as defined by the Act;

ii. conform with a specific framework or publication listed in the Act (such as NIST special publications);

iii. for personal information regulated by a government entity, conform with requirements of applicable regulations including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and Utah's Protection of Personal Information Act; or

iv. (iv) for personal information protected by the Payment Card Industry Data Security Standard, conform with the requirements of the PCI data security standards.

*Id.* § 78B-4-703(1)(b)(iii).

Perhaps most important is the Act's recognition that there is no "one size fits all" solution by providing that the program should be "of an appropriate scale and scope" taking into consideration the entity's size and complexity, the nature and scope of its activities, the sensitivity of the information, the cost and availability of tools "to improve information security and reduce vulnerability," and "the resources available to the person." *Id.* § 78B-4-702(4)(c). This scalability component provides much needed relief to those that have postponed addressing cybersecurity simply because the task seemed too daunting for a small entity to undertake.

Of course, a cybersecurity program must actually be *implemented and enforced* by ensuring that employees are properly trained, and enforced. And, an entity that ignores a known threat or hazard to its system and fails to act in a reasonable time cannot claim the defense.

With data breaches and ransomware on the rise, there is no better time to update or implement a robust, thorough cybersecurity program to take advantage of Utah's new "safe harbor."

*Ms. Maragakis is a shareholder and director and practices in Ray Quinney & Nebeker's litigation section. Her practice focuses on complex commercial litigation. Ms. Maragakis has represented a number of health care entities, including nursing homes and hospitals, in litigation, HIPAA analysis, and medical staffing issues. Ms. Maragakis is also Chair of the Firm's Cybersecurity and Privacy practice group. Ms. Maragakis has obtained her designation as a Certified Information Privacy Professional/US (CIPP/US), a certification offered by the International Association of Privacy Professionals. She assists clients in all aspects of legal compliance with data security laws, including preparing cybersecurity programs, Data Breach Response Plans and Employee Data Security Policies.*

1 This article is intended as a summary on the Act, and is not legal advice. Consult an attorney for specific guidance.

2 The Act defines a "Person" as an individual, an association, a corporation, a joint stock company, a partnership, a business trust, or any unincorporated organization. Utah Code Ann. 78B-4-701(4)(a). For ease of reference, this article uses the term "entity" to encompass the definition of a "Person."

3 Comments in House Business and Labor Committee (2/8/2021).