wiley

NEWSLETTER

Utah Establishes a Legal Safe Harbor for Companies That Adopt Data Security Programs

April 2021

Privacy In Focus®

Utah has become the second state to establish a legal safe harbor for private-sector entities that follow certain cybersecurity best practices. On March 11, 2021, Utah's Governor Spencer Cox signed into law the Cybersecurity Affirmative Defense Act, H.B. 80, which provides an affirmative defense for companies that create, maintain, and reasonably comply with a written cybersecurity program, but that are nonetheless victims of a data security breach. Seen largely as an effort to incentivize the voluntary adoption of robust data security practices, the bill follows a similar law enacted in Ohio in 2018, but departs from the Ohio model in a number of significant ways.

The Utah Law Creates Three Distinct Affirmative Defenses Available to Companies that Have Implemented Written Cybersecurity Programs.

Specifically, H.B. 80 provides an affirmative defense to three claims: (1) failure to implement reasonable information security controls; (2) failure to appropriately respond to a breach; and (3) failure to appropriately notify individuals whose personal information was compromised. To avail itself of these affirmative defenses, a company must have a written cybersecurity program that meets certain requirements, including having a cybersecurity program in place at the time of the breach that reasonably conforms to a recognized cybersecurity framework. In addition, to avail itself of the latter two affirmative defenses – which deal with response and notification following a breach – a company must have had in place certain

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

relevant protocols at the time of the breach.

The law also includes a severability clause and provides that, where applicable, a choice of law provision in an agreement that designates Utah as the governing law will apply the law regardless of where the civil action is brought.

To Take Advantage of the Safe Harbor, Companies' Cybersecurity Programs Must Satisfy Several Conditions, Including Reasonably Conforming to a Recognized Cybersecurity Framework.

First, to avail itself of one of the affirmative defenses, a company's written cybersecurity program must provide administrative, technical, and physical safeguards to protect personal information, including being designed to:

- Protect the security, confidentiality, and integrity of personal information;
- Protect against any anticipated threat or hazard to the security, confidentiality, or integrity of personal information; and
- Protect against a breach of system security.

Second, as a condition of the safe harbor, the written cybersecurity program must reasonably conform to one of several recognized cybersecurity frameworks, or a combination thereof. The recognized cybersecurity frameworks include NIST Special Publication 800-171; NIST Special Publications 800-53 and 800-53a; the FedRAMP Security Assessment Framework; the Center for Internet Security Critical Security Controls for Effective Cyber Defense; and the ISO 27000 family of standards, among others. Notably, the Utah law does not identify the NIST Cybersecurity Framework as a stand-alone "recognized cybersecurity framework," which is a departure from the Ohio law.

Third, the new Utah law requires that – for a company to take advantage of the safe harbor – its written cybersecurity program must have an appropriate scale and scope, considering:

- A company's size and complexity;
- The nature and scope of its activities;
- The sensitivity of the information to be protected;
- The cost and availability of tools to improve information security and reduce vulnerability; and
- The company's resources.

Fourth, the written program must be a "reasonable security program," which the law describes as including, among other things, practices and procedures to detect, prevent, and respond to breaches, including by conducting risk assessments.

Utah Will Not Allow the Affirmative Defense if a Company Had Actual Notice of the Threat and Did Not Act Within a Reasonable Amount of Time to Remediate It.

In another departure from the Ohio law, H.B. 80 provides that a company may not claim an affirmative defense if the company (1) had actual notice of the threat or hazard; (2) did not act in a reasonable amount of time to take known remedial efforts against such threat or hazard; *and* (3) the threat or hazard resulted in the breach. Importantly, the law clarifies that a risk assessment to improve security is *not* "actual notice of a threat or hazard."

Looking Forward

Utah's safe harbor law does not provide rigid requirements for what cybersecurity protections will be considered "reasonable," and leaves companies considerable flexibility in how they adopt the various cybersecurity frameworks. Rather, Utah's safe harbor law builds on the expectation that companies should likely have a developed, written cybersecurity program that at least considers one of the many available frameworks. Further, other states are considering similar safe harbor laws, and the experience of early adopters like Utah and Ohio will inform what those laws look like – and may eventually inform what will be considered a baseline cyber standard of care going forward.

Wiley's Privacy, Cyber & Data Governance Team has helped entities of all sizes from various sectors proactively address risks and address compliance with new cybersecurity laws. Please reach out to any of the authors with questions.