Utah Code Ann. § 78B-4-702

Current through May 1, 2024 of the 2024 General Session.

Utah Code Annotated > Title 78B Judicial Code (§§ 78B-1-101 — 78B-25-115) > Chapter 4 Limitations on Liability (Pts. 1 — 7) > Part 7 Cybersecurity Affirmative Defense Act (§§ 78B-4-701 — 78B-4-706)

78B-4-702. Affirmative defense for a breach of system security.

(1) A person that creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (4), 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 the person failed to implement reasonable information security controls that resulted in the breach of system security.

(2) A person has an affirmative defense to a claim that the person failed to appropriately respond to a breach of system security if:

(a) the person creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (4) and is in place at the time of the breach of system security; and

(b) the written cybersecurity program had protocols at the time of the breach of system security for responding to a breach of system security that reasonably complied with the written cybersecurity program under Subsection (2)(a) and the person followed the protocols.

(3) A person has an affirmative defense to a claim that the person failed to appropriately notify an individual whose personal information was compromised in a breach of system security if:

(a) the person creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (4) and is in place at the time of the breach of system security; and

(b) the written cybersecurity program had protocols at the time of the breach of system security for notifying an individual about a breach of system security that reasonably complied with the requirements for a written cybersecurity program under Subsection (3)(a) and the person followed the protocols.

(4) A written cybersecurity program described in Subsections (1), (2), and (3) shall provide administrative, technical, and physical safeguards to protect personal information, including:

(a) being designed to:

(i) protect the security, confidentiality, and integrity of personal information;

(ii) protect against any anticipated threat or hazard to the security, confidentiality, or integrity of personal information; and

(iii) protect against a breach of system security;

(b) reasonably conforming to a recognized cybersecurity framework as described in Subsection 78B-4-703(1); and

(c) being of an appropriate scale and scope in light of the following factors:

(i) the size and complexity of the person;

(ii) the nature and scope of the activities of the person;

(iii) the sensitivity of the information to be protected;

(iv) the cost and availability of tools to improve information security and reduce vulnerability; and

(v) the resources available to the person.

(5)

(a) Subject to Subsection (5)(b), a person may not claim an affirmative defense under Subsection (1), (2), or (3) if:

(i) the person had actual notice of a threat or hazard to the security, confidentiality, or integrity of personal information;

(ii) the person did not act in a reasonable amount of time to take known remedial efforts to protect the personal information against the threat or hazard; and

(iii) the threat or hazard resulted in the breach of system security.

(b) A risk assessment to improve the security, confidentiality, or integrity of personal information is not an actual notice of a threat or hazard to the security, confidentiality, or integrity of personal information.

History

2021 ch. 40, § 2, effective May 5, 2021.