BILL ANALYSIS

S.B. 2610
By: Blanco
Delivery of Government Efficiency
Committee Report (Unamended)

BACKGROUND AND PURPOSE

The bill sponsor has informed the committee that cyberattacks impose a staggering financial toll on American businesses, with small and medium-sized businesses being the most vulnerable targets due to their limited budgets, staff, and technical expertise to implement sophisticated cybersecurity defenses. The bill sponsor has also informed the committee that these attacks can damage small businesses through direct losses like stolen funds, indirect costs such as prolonged operational downtime, and lasting reputational harm that erodes customer trust and threatens both short-term functionality and long-term survival.

S.B. 2610 addresses this issue by establishing a legal "safe harbor" for certain businesses that proactively adopt recognized cybersecurity frameworks, offering them protection from punitive lawsuits in the event of a breach. By incentivizing investment in certain recognized cybersecurity frameworks and best practices, the bill encourages a proactive approach to safeguarding sensitive consumer data, including personal and payment information. Through these measures, S.B. 2610 seeks to bolster Texas' economic resilience, reduce burdens on small businesses, and enhance consumer confidence in the state's marketplace.

CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

RULEMAKING AUTHORITY

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

ANALYSIS

S.B. 2610 amends the Business & Commerce Code to prohibit a person harmed from a breach of system security from recovering exemplary damages in an action arising from the breach from a business entity in Texas that has fewer than 250 employees and owns or licenses computerized data that includes sensitive personal information if the entity demonstrates that at the time of the breach the entity implemented and maintained a cybersecurity program that meets the following criteria:

- contains administrative, technical, and physical safeguards for the protection of personal identifying information and sensitive personal information;
- conforms to an industry-recognized cybersecurity framework as described by the bill;
- is designed to protect the security of personal identifying information and sensitive personal information, protect against any threat or hazard to the integrity of such information, and protect against unauthorized access to or acquisition of such information that would result in a material risk of identity theft or other fraud to the individual to whom the information relates; and

- with regard to the scale and scope, meets the following requirements:
    - for a business entity with fewer than 20 employees, simplified requirements, including password policies and appropriate employee cybersecurity training;
    - for a business entity with at least 20 employees but fewer than 100 employees, moderate requirements, including the requirements of the Center for Internet Security Controls Implementation Group 1; and
    - for a business entity with at least 100 employees but fewer than 250 employees, compliance with the requirements of an industry-recognized cybersecurity framework as described by the bill.

S.B. 2610 establishes that such a cybersecurity program conforms to an industry-recognized cybersecurity framework for purposes of the bill's provisions if the program conforms to the following:

- a current version of or any combination of current versions of the following:
    - the Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology (NIST);
    - the NIST's special publication 800-171;
    - the NIST's special publications 800-53 and 800-53a;
    - the Federal Risk and Authorization Management Program's FedRAMP Security Assessment Framework;
    - the Center for Internet Security Critical Security Controls for Effective Cyber Defense;
    - the ISO/IEC 27000-series information security standards published by the International Organization for Standardization and the International Electrotechnical Commission;
    - the Health Information Trust Alliance's Common Security Framework;
    - the Secure Controls Framework;
    - the Service Organization Control Type 2 Framework; or
    - other similar frameworks or standards of the cybersecurity industry;
- if the business entity is subject to its requirements, the current version of the following federal laws:
    - the Health Insurance Portability and Accountability Act of 1996;
    - Title V of the Gramm-Leach-Bliley Act;
    - the Federal Information Security Modernization Act of 2014; or
    - the Health Information Technology for Economic and Clinical Health Act; and
- if applicable to the business entity, a current version of the Payment Card Industry Data Security Standard.

The bill establishes that if any standard in this list, not including the federal laws or the Payment Card Industry Data Security Standard, is published and updated, a business entity's cybersecurity program continues to meet the requirements of such a program under the bill if the entity updates the program to meet the updated standard not later than the later of the implementation date published in the updated standard or the first anniversary of the date on which the updated standard is published.

S.B. 2610 establishes that its provisions may not be construed to create a private cause of action or change a common law or statutory duty. The bill applies only to a cause of action that accrues on or after the bill's effective date.

S.B. 2610 defines the following terms for purposes of its provisions:

- "breach of system security" has the meaning assigned by Business & Commerce Code provisions relating to required notification following a breach of security of computerized data;
- "exemplary damages" has the meaning assigned by Civil Practice and Remedies Code provisions relating to damages; and
- "personal identifying information" and "sensitive personal information" have the meanings assigned by the Identity Theft Enforcement and Protection Act.

EFFECTIVE DATE

September 1, 2025.