SpencerFane

Texas Cybersecurity Safe Harbor for Small and Mid-Sized Businesses

Texas has taken a significant step toward incentivizing cybersecurity best practices for small and mid-sized businesses. Senate Bill 2610, effective September 1, 2025, creates a legal safe harbor for companies that adopt recognized cybersecurity frameworks. This law is designed to reduce punitive damages exposure in lawsuits arising from data breaches, while encouraging proactive security measures.

Why This Matters

Data breaches are costly – not just in terms of remediation and reputational harm, but also in litigation risk. SB 2610 offers businesses a way to mitigate that risk by aligning with industry standards. For organizations that handle sensitive personal information, this is an opportunity to strengthen defenses and gain legal protection.

Key Provisions of SB 2610

- *Scope*: Applies to Texas businesses with fewer than 250 employees that own or license computerized data containing sensitive personal information.
- *Safe Harbor Criteria*: Businesses must maintain a documented cybersecurity program that includes administrative, technical, and physical safeguards and conforms to recognized frameworks such as NIST CSF, ISO/IEC 27001, or CIS Controls.
- *Tiered Requirements*:
  - Fewer than 20 employees: Basic measures like password policies and employee training.
  - 20-99 employees: CIS Controls Implementation Group 1.

    - 100-249 employees: Full compliance with advanced frameworks like NIST CSF or ISO/IEC 27001.
- *Legal Effect*: Compliance shields businesses from punitive damages in breach-related lawsuits, though compensatory damages and regulatory enforcement remain unaffected.

Effective Date

SB 2610 was signed into law on June 20, 2025, and became effective September 1, 2025.

Practical Impact

This law does not impose new regulatory mandates but provides a strong incentive for SMBs to adopt cybersecurity standards. It rewards proactive measures and reduces financial risk, making compliance a strategic advantage.

What Businesses Should Do Now

- Assess whether SB 2610 applies to your organization.
- Select and implement an appropriate cybersecurity framework based on your size.
- Document policies, training, and technical safeguards.
- Conduct annual reviews and maintain evidence of compliance.

Spencer Fane Can Help

Our team advises businesses on cybersecurity compliance and risk management. If you have questions about SB 2610 or need assistance implementing a framework, contact us today.

This blog was drafted by Shawn Tuma, an attorney in the Spencer Fane Plano, Texas office and the leader of the firm's Cyber | Data | Artificial Intelligence | Emerging Technology team. For more information, visit www.spencerfane.com.

Click **here** to subscribe to Spencer Fane communications to ensure you receive timely updates like this directly in your inbox.