CYBERSECURITY AWARENESS MONTH

STATE OF TEXAS INTENSIFIES ITS PROBES INTO CYBERSECURITY NON-COMPLIANCE

by Lynn Rohland,
Gray Reed Advisory Principal

A concerning trend has emerged among businesses in the state of Texas following the passage of the Texas Data Privacy and Security Act (TDPSA) on July 1, 2024. Companies appear to be courting disaster by overlooking – or brazenly sidestepping – critical compliance mandates. Initially hailed as a 'privacy law' modeled after Virginia and California state laws, the TDPSA mandates cybersecurity requirements as much as it establishes privacy expectations for how consumer data is handled. Therein lies the problem: businesses are treading on dangerous ground by neglecting or falling short of demonstrating cybersecurity compliance, raising the risk of scrutiny by the Texas Attorney General's (AG) Office and incurring costly implications.

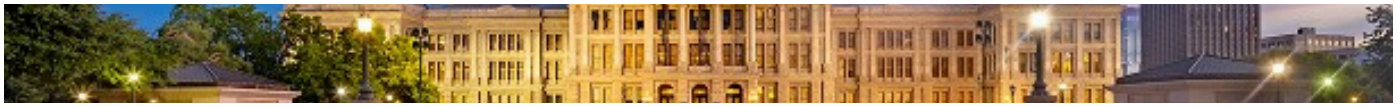
For instance, on September 3, 2025, the Texas Attorney General's (AG) Office filed a lawsuit against PowerSchool, a cloud-based education software provider, following a December 2024 data breach affecting more than 880,000 Texas students and teachers.

. The complaint alleges violations of the TDPSA for failing to implement basic IT security protections, including multi-factor authentication, access controls, and data encryption, which allowed hackers to exploit a third-party subcontractor's login credentials and abscond with unencrypted sensitive data, including Social Security numbers and medical records, to a foreign server. The AG is seeking penalties of up to $7,500 per violation as well as multimillion-dollar fines for deceptive claims about platform security.

This is not the first time the AG has sued entities for non-compliance with the TDPSA's security provisions under Section 541.101. Earlier this year, the Texas AG sued a Fortune 500 insurance company and its subsidiary for violations of the TDPSA. The lawsuit alleged the two companies embedded tracking software into third-party mobile apps to collect precise geolocation data and driving behavior on millions of Texans without obtaining their consent or providing adequate notice.

Impacts of Falling Short

The TDPSA applies to any entity conducting business in Texas or delivering products or services to Texas residents that collects, processes, or sells personal data. However, certain exemptions apply, including if an entity is a state agency, non-profit, institute of higher education, electric or power company, or is governed by the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA), or deemed a small business (as defined by the U.S. Small Business Administration).



It also mandates that businesses implement "reasonable administrative, technical, and physical data security practices" to protect the confidentiality and integrity of their data. Those found non-compliant can incur fines of up to $7,500 per violation, with a 30-day cure period, which means a company has one opportunity to remediate compliance gaps and a very short runway to do so. Since the law's security provisions are not overly prescriptive, many chief information officers (CIOs) and risk and compliance officers ask, "How do we know when we're compliant?" Clearly, there's no sympathy for the lack of specificity, given the AG's enforcement actions in 2025.

Navigating Vague Security Obligations

Under Section 541.101 of the TDPSA, businesses that own (aka Controllers) or process (aka Processors) personal data are required to:

1. Limit the collection of personal data (aka' data minimization') to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that data is processed, and disclosed to the consumer.
2. Establish, implement, and maintain reasonable administrative, technical, and physical data security practices specifically designed to protect the confidentiality, integrity, and accessibility of personal data.
3. Safeguard personal data against threats such as unauthorized access, use, disclosure, or other harm that could affect consumers, aligning with broader data protection goals under the TDPSA.

While a host of controls and measures can be explored, let's focus on a couple of the basic, blocking-and-tackling components a company of any size should have in place to help demonstrate compliance with Section 541.101.

CYBERSECURITY AWARENESS MONTH

Data Minimization

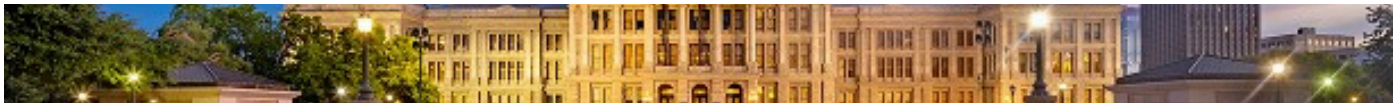
At the heart of today's cybersecurity issues is understanding what data you have, including where it is located, who has access to it, for what purposes, and how it is being safeguarded. That's where data inventories can be extremely useful to ensure data minimization, because tracking the details about personal data collected, processed, stored, and shared can serve as a vital 'source of truth' to demonstrate use limitation, as well as to audit and correct business data collection practices found to be noncompliant.

Although TDPSA does not require data inventories, they are invaluable tools during cyberattacks, data breaches, system migrations, mergers and acquisitions, or when determining the security required for specific types of data, ultimately dictating the security controls to be deployed.

Common Security Controls

Probably one of the most critical success factors, and a great starting point for any business, is to adopt and implement an IT security or cybersecurity framework. There are many frameworks to choose from, and most prescribe the specific controls and measures needed to implement administrative, technical, and physical security while helping to govern, identify, protect, detect, respond, and recover from cybersecurity threats, vulnerabilities, and risks. Two of the most widely recognized and adopted frameworks are the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) and the International Organization for Standardization's 27001, Information Security Management Systems (ISMS) — Requirements (ISO/IEC 27001).

CYBERSECURITY AWARENESS MONTH

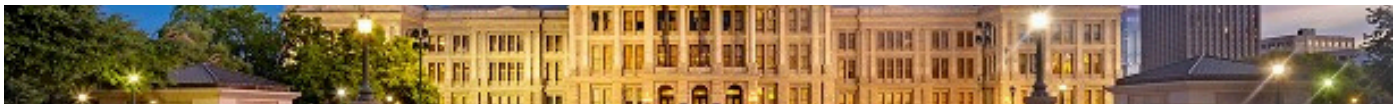


Adopting a framework will not only assist a business in understanding what controls are necessary to comply with the TDPSA, but also in building out its cyber capabilities while using a repeatable and scalable construct to operate, manage, and continuously monitor its practices.

Finally, a conversation on the types of tools available to mitigate the threats of unauthorized access, use, or disclosure of personal data can be vast, wide-ranging, and potentially complex. That said, considering the current cyber landscape, most businesses have implemented the following technologies and countermeasures:

- Identity and Access Management tools to enforce role-based access and multi-factor authentication.
- Encryption software for use with data at rest and data in transit.
- Intrusion Detection and Prevention Systems to monitor network traffic for suspicious activity and alert or block unauthorized access attempts.
- Data Loss Prevention tools to scan and block unauthorized sharing of personal data via email, uploads, or onto USB devices.
- Endpoint Detection and Response technologies to provide continuous monitoring and automated responses to external or insider threats.
- Security Information and Event Management systems to detect anomalies and facilitate swift investigation of unauthorized use or access incidents.

CYBERSECURITY AWARENESS MONTH



How We Help Clients

While the cyber mandates are arguably non-prescriptive to offer flexibility, it should not be misconstrued that these provisions are any less critical or would not be scrutinized by the AG should your business incur a cyberattack. Instead, the law provides businesses with the ability to right-size their cybersecurity needs based on the types of personal data collected or processed, the size of operations, industry sector, and current operating model.
If you're falling short of compliance mandates, there's still time, but the runway is short.

Our team helps businesses assess risks, close compliance gaps, and build cybersecurity and data privacy programs tailored to your operations. Now is the time to take proactive steps—our team is ready to guide you toward compliance and stronger cyber resilience.