The Texas Cybersecurity Act
HB8 by Rep. Giovanni Capriglione

With a reliance on digitally connected infrastructure and markets, the world is experiencing an unprecedented threat to individual privacy and personal information. Cyber theft and related crime affects every part of our economy, our government, and our daily lives. The State of Texas must lead the way in developing a holistic cybersecurity strategy for our state agencies that will complement the foundation measures currently in place. Texas must be prepared and must remain vigilant.

To that end, HB 8 defines and establishes The Texas Cybersecurity Act which will enhance and better equip our state's cybersecurity programs.

Some high points of the legislation include:

- The creation of a cyber sharing task force allowing legislative and information technology leaders to confer and synthesize existing resources and best practices to construct cybersecurity measures that work best for the state.
- The Department of Information Resources (DIR) may join into agreement with organizations such as the National Cybersecurity Preparedness Consortium and institutions of higher education to support DIR's efforts in addressing cybersecurity risks and incidents in the state.
- A review of an agency's cybersecurity practices will be included in their Sunset process.
- The creation of a House Select Committee on Cybersecurity and Senate Select Committee on Cybersecurity.
- The creation of three evaluations:
    - The Homeland Security Council will conduct a detailed report on cyber attacks on state agencies.
    - The Texas Rangers will investigate vulnerabilities in election infrastructure.
    - DIR and the Texas State Library and Archives Commission (TSLAC) will review state agency digital data storage, their records management practices, and the associated cost to the state.
- State agencies must:
    - Notify their Chief Information Security Officer and the State Cybersecurity Coordinator if a breach, suspected breach, or unauthorized exposure is discovered within 48 hours.
    - Require their executive head and Chief Information Security Officer review their information security plan and strategies for addressing their highest risk for breaches annually and approve in writing.
    - Contract with an independent third party to audit each agency's security risks at least every five years and report the results to the legislature.
    - Destroy personally identifiable information if not required by another law to retain.
    - Ensure they are using the most efficient and secure cloud service available to them.
    - Adopt the cybersecurity framework core functions written by the National Institute of Standards and Technology (NIST): Identify, Protect, Detect, Respond, and Recover.
    - Establish mandatory guidelines for cybersecurity certification by all information resource employees of each agency.

Paid for by the Texas Business Leadership Council
515 Congress Avenue, Suite 1780 | Austin, TX 78701 | Phone (512) 481-0525