THE TEXAS CYBERSECURITY ACT - HB8

BY GIOVANNI CAPRIGLIONE
JOINT AUTHORS: GARY ELKINS, TAN PARKER, TONY DALE, JAY DEAN
COAUTHORS: TERRY CANALES, CRAIG GOLDMAN, MATT KRAUSE

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.

Committee substitute changes on back.

SUPPORTED BY: **TEXAS BUSINESS LEADERSHIP COUNCIL | TEXAS ASSOCIATION OF BUSINESS | TEXAS ASSOCIATION OF MANUFACTURERS | TECHNET**

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

HB 8 COMMITTEE SUBSTITUTE CHANGES

- Allows local governments that same authority to discuss cybersecurity issues in closed session as enjoyed by DIR.
- Adds provision for state employee cybersecurity training.
- Clarifies "vendor responsibility for cybersecurity."
    - Must demonstrate that all data provided by the State to the vendor will be maintained in compliance with all state and federal laws and regulations, to the extent that they apply.
    - Defines "known cybersecurity risk."
    - Clarifies that known cybersecurity risks will be identified in the vulnerability and penetration test.
- Authorizes an allotment for appropriate industry-recognized certification exams to state and local officials and first responders preparing for and responding to cybersecurity risks and incidents.
- Adds routine cyber hygiene training to state agency personnel with access to state agency networks in order to mitigate cybersecurity risks and vulnerabilities.
- Cybersharing task force must assess the knowledge, skills, and capabilities of the existing workforce and develop recommendations for addressing immediate workforce gaps and ensuring a long-term talent pipeline.
- Adds that cybersecurity training must be industry-recognized, and these certifications must be included in the state agency cybersecurity plan.
- Cybersecurity task force may hire a vendor to assist the task force in planning and bringing in best practices.
- Amends definitions of "cyberattack" and "cybersecurity risks."
- Changes "cost-effective" to "best value" for replacing legacy systems.
- Standardizes agency incident response plans.
- Allows DPS to contract out for cybersecurity plans.
- Adds that if an agency is not subject to TSLAC record retention policies, they must destroy sensitive data unless for law enforcement purposes.
- The Sunset Advisory Commission may use DIR's cybersecurity report to determine effectiveness of mission instead of doing their own separate report.
- Clarifies "data security plan" section.
    - Does not apply to institutions of higher education. Each of these institutions shall adopt and implement a policy governing Internet website and mobile application security procedures that complies with this section.
    - Requires agencies to have a security plan and perform systems scans for new systems. The responsibility is placed on the agency, not external organizations like DIR.
    - The vulnerability assessment will be risk based so that only "high" priority vulnerabilities will stop going live. "Medium" and "low" are at the discretion of the agency.
- Directs the Secretary of State to conduct the study on election cyberattacks instead of the Texas Rangers.
- Cyber risk sign-off must be performed by an agency's executive head and ISO (or CISO, if applicable). The executive head is responsible for all risk incurred.