TEXAS BUSINESS LEADERSHIP COUNCIL

2017 LEGISLATIVE RECOMMENDATIONS

CYBER SECURITY

Cyber security risk is a policy-level issue to be handled at the elected and appointed official level, not just administratively at an agency or within information technology departments at agencies. In the private sector, cyber security risk has been elevated to a Board of Directors and CEO issue. The equivalent should happen within the State of Texas, from the Governors office, to the legislature, and at the appointed policy level within state agencies.

States like South Carolina and Utah have experience major security breaches that involved spending millions of dollars to restore citizen trust. The State of Texas should take action to both prevent and prepare for such a scenario.

While multiple issues need to be addressed one principal concern is that there is not a central legislative committee responsible for cyber security risk issues in the Texas legislature. Unlike the US House of Representatives and Senate, where there are multiple committees and sub committees responsible for issues around cyber security, there is not one House or Senate Committee in Austin that solely addresses cyber security issues. An overarching recommendation to the six priority issues included herein is that both the Lt. Governor and the Speaker of the House create committees in the 2017 legislative session to adequately address public policy issues surrounding cyber security and privacy.

The Texas Business Leadership Council has created a Cyber Security Task Force comprised of expert individuals from the private sector (roster included below). The Task Force has developed, and the TBLC has adopted, the public policy recommendations that follow.

CYBER SECURITY LEGISLATIVE RECOMMENDATIONS

Ensure Agency Executives Make Cyber Risk Sign-offs
The TBLC recommends legislation be enacted which enforces Texas Administrative Code (TAC) 202, providing that agency leaders sign-off on all cyber risks for their agencies. Further, the sign-off documents should be filed with the Legislative Budget Board (LBB) prior to the agency's consideration for Legislative Appropriation Requests (LARs).

Although mandated by TAC 202, state agency heads do not consistently sign-off on cyber security risks, nor do legislative branch leaders receive updates that sign-offs have occurred. The TBLC recommends that the legislature enforce TAC 202 by tying cyber security sign offs and legislative reporting to LARs made by each agency. All agency heads (elected or appointed) and their Chief Information Security Officers should sign off-on cyber security risk within their organizations on an annual basis. This action will increase accountability across all state agencies, and when cyber security breaches occur, the correct executive leader will more likely be held responsible by the public.

Move Agency Security Out of the Chain of Command of the CIO
The TBLC recommends that within applicable executive branch agencies, it be required that division of labor ensures that the Chief Information Security Officer (CISO) works independently in terms of organizational structure and budget from the IT division.

A leading practice in the commercial sector, the CISO must be independent of the CIO. Too often, the budget constraints of IT lead to sub-optimization of investment in cyber security within organizations where the CISO reports to the CIO. In addition, when the CISO is supposed to hold the IT department accountable for the cyber security posture of the organization, it is challenging when the CISO is subordinated to the leader of the IT department. The structure at the Texas Comptroller of Public Accounts is what we see often in commercial organizations. CISOs report to the CFO, Chief Risk Officer, or Chief of Staff.

Further Integration of Secure Cloud Storage Data Solutions
The TBLC recommends that the State of Texas review current guidelines dictating data that is allowed to be stored on the cloud versus state data storage systems.

With innovations in technology and advancements in the capacity of private and secure cloud storage systems, it would be prudent for the State of Texas to review options for systems that would be more affordable, secure, and efficient to the state.

CYBER SECURITY LEGISLATIVE RECOMMENDATIONS

Perform State Agency Risks Assessments
The TBLC recommends that State of Texas agencies be required to perform independent risk assessments to quantify their cyber security exposure and report back to the legislature or appropriate executive branch agency.

States including Utah, Michigan, and New York have all procured independent, enterprise wide security assessments conducted by 3rd parties. The benefits over self-assessment include a much more realistic evaluation of the security posture of the organization and the ability to identify systemic/pervasive commonalities of vulnerabilities across agencies that potentially can be addressed by state-wide initiatives. The application of a common approach and consistency is important to understand the security posture across agencies.

Move to Eliminate Risk of Private Citizen Data on Legacy Systems
The TBLC recommends that the legislature act to reduce the level of exposure that State of Texas agencies have regarding private citizen data housed on public legacy systems.

The State of Texas must ensure that agency legacy systems, particularly systems that are end-of-life / out of date, do not contain sensitive citizen data that could result in data breaches due to inadequate protection. Further, the legislature should determine the most cost effective approach to updating/disposing those systems housing mission critical data (replacement, incremental renewal, re-platforming, decommission of equipment and outsourcing data, etc.).

Conduct Privacy Impact Assessments for New Self-Service Functions
The TBLC recommends that prior to beta testing any online or mobile application which processes a citizen's personally identifiable information or information attributes that would be classified as confidential; all agencies must submit a data security plan to the legislature or appropriate executive branch agency.

The legislature or appropriate executive branch agency will review the plan to include; data flow diagrams (data in use, in transit, and at rest), data storage, data interaction with mobile devices, idata transfer security, among other mobile and best-practice web/mobile application development security measures. The legislature or appropriate executive branch agency should require that all internet-facing websites, applications and mobile portals undergo a 3rd party vulnerability and penetration test and all findings be remediated prior to deployment.

CYBER SECURITY PROCEDURAL RECOMMENDATION

Create Legislative Committees for Cyber Security

The TBLC recommends that the Lt. Governor and Speaker of the House create standing committees on cyber security in each chamber (or alternatively, a joint select committee or standing sub-committees) with the sole purpose of addressing public policy issues surrounding cyber security and privacy risk as it relates to state agencies.

Currently, multiple committees in both the Senate and House have jurisdiction over cyber security and privacy matters. A more coordinated approach will provide clear guidance and proper oversight for state agencies and enable state agencies to follow a more direct path to improve their cyber security activities in a more consistent fashion.

TEXAS BUSINESS LEADERSHIP COUNCIL

TBLC Cyber Security Task Force Roster

John Dickson, Chairman & TBLC Member
The Denim Group

Eric Hames
The Frontline Group

Jeffrey Julig
SWBC

Bill Lines
PlainsCapital Bank

Geoffrey Parsons
Baylor Scott & White Health

James Phillippe
Ernst & Young LLP

Patrick Reinhart
El Paso Electric

Michael Wyatt
Deloitte & Touche LLP

For additional information please contact:
Justin Yancy
President
Texas Business Leadership Council
515 Congress Ave., Suite 1780
Austin, Texas 78701
(512) 481-0525
yancy@txblc.org

@tx_blc /txblc