SUBJECT: Creating cybersecurity-related requirements for state agencies

COMMITTEE: Government Transparency and Operation — committee substitute recommended

VOTE: 7 ayes — Elkins, Capriglione, Gonzales, Lucio, Shaheen, Tinderholt, Uresti

0 nays

WITNESSES: For — Sarah Matz, CompTIA; Justin Yancy, Texas Business Leadership Council; (*Registered, but did not testify*: Edward Henigin, Data Foundry, Inc.; Fred Shannon, Hewlett Packard; Wendy Reilly, HID Global; Buddy Garcia, NEC America; Juan Antonio Flores, Port San Antonio, San Antonio Chamber of Commerce; Vincent Giardino, Tarrant County Criminal District Attorney's Office; Caroline Joiner, TechNet; Amanda Martin, Texas Association of Business; Stephanie Simpson, Texas Association of Manufacturers; Michael Goldman, Texas Conservative Coalition; Nora Belcher, Texas e-Health Alliance; Karen Robinson, Texas Technology Consortium; Thomas Parkinson)

Against — None

On — (*Registered, but did not testify*: Todd Kimbriel, Department of Information Resources; Aaron Blackstone and Bryan Lane, Department of Public Safety; Charlotte Willis, Health and Human Services Commission; Sacha Jacobson)

BACKGROUND: Government Code, sec. 2054.133 requires each state agency to develop an information security plan for protecting the security of the agency's information.

Sec. 2054.1125 requires a state agency to disclose any breach of system security as soon as possible to any individual whose sensitive personal information was or is believed to have been compromised.

DIGEST:

CSHB 8 would establish the Texas Cybersecurity Act. It would create certain cybersecurity-related requirements for all state agencies, establish a cybersecurity task force and select legislative committees, and require the production of certain studies and reports.

Cybersecurity task force. CSHB 8 would require the Department of Information Resources (DIR) to establish and lead a cybersecurity task force that included representatives of state agencies, including institutions of higher education, to engage in policy discussions and educate state agencies on cybersecurity issues. The task force would have certain duties, including:

- consolidating and synthesizing existing cybersecurity resources and best practices;
- assessing the knowledge, skills, and capabilities of the existing information technology (IT) and cybersecurity workforce;
- developing guidelines on cyber threat detection and prevention,
- recommending legislation to implement remediation strategies for state agencies; and
- providing opportunities for state agency technology leaders and members of the Legislature to participate in programs and webinars on cybersecurity policy issues.

The task force would be abolished on September 1, 2019, unless extended until September 1, 2021.

Plan to address cybersecurity risks and incidents. The Department of Public Safety (DPS) would be required to develop a plan to address cybersecurity risks and incidents. To develop the plan, the department could partner with a national organization and enter into an agreement that could include provisions to:

- develop and maintain a cybersecurity risks and incidents curriculum and conduct training and simulation exercises for state agencies, political subdivisions, and private entities to encourage coordination in defending against and responding to risks and

incidents;

- provide technical assistance services to support preparedness for and response to cybersecurity risks and incidents; and
- incorporate cybersecurity risk and incident prevention and response methods into existing state and local emergency plans.

In implementing the agreement, the department would be required to avoid unnecessary duplication of its or another agency's existing programs or efforts and consult with institutions of higher education.

Information sharing and analysis center. The bill would require DIR to establish and administer a center for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies. Persons from appropriate state agencies and the cybersecurity task force would be appointed as representatives to the center.

Information security plan. The bill would require the executive head and chief information security officer of each state agency to review annually and approve in writing the agency's information security plan. The executive head would retain full responsibility for the agency's information security and any risks to that security. An agency would have to file the written approval before submitting a legislative appropriation request.

In addition to what already is included in an information security plan, the bill would require an agency to provide steps taken to identify any information individuals had to provide or that the agency retained that was not necessary for the agency's operations. The plan also would have to include privacy and security standards that require a vendor offering cloud computing services or other IT solutions to demonstrate that data provided to the vendor would be maintained in compliance with state and federal law.

Independent risk assessment. At least once every five years, a state agency would be required to contract with a DIR-recommended independent third party to conduct a risk assessment of the agency's

exposure to security risks and practice actions in the event of a breach.

The results of this assessment would be submitted to DIR, which would prepare an annual public report on the general security issues and an annual confidential report on specific risks and vulnerabilities. DIR also would have to submit an annual comprehensive report to the Legislature providing recommendations to address any identified vulnerabilities.

Meetings to deliberate security devices or audits. The bill would permit all governmental bodies, not only DIR as under current law, to conduct a closed meeting to deliberate security assessments of information resources technology, network security information, or the deployment of personnel, critical infrastructure, or security devices.

Vulnerability reports. The bill would require, rather than permit as under current law, the information resources manager of a state agency to prepare or have prepared a report assessing the extent to which information technology of the agency was vulnerable to unauthorized access or harm.

Data security procedures for online and mobile applications. Except for institutions of higher education, each state agency with a website or mobile application that processes personally identifiable or confidential information would have to submit a data security plan to DIR during development and testing that included relevant security information defined in the bill.

Institutions of higher education would have to submit to DIR a policy for website and mobile application security procedures that included certain requirements for website or application developers.

Each agency would be required to subject a website or application to a vulnerability and penetration test prior to deployment.

Individual identifying information. A state agency would be required to destroy personally identifiable information if the agency was not

statutorily required to retain the information for a period of years and develop policy to do so by September 1, 2019. This provision would not apply to a record involving a criminal activity or investigation retained for law enforcement purposes.

Security breach notification. A state agency that handled computerized data that included sensitive personal information would have to notify DIR within 48 hours after the discovery of a breach or suspected breach of system security or unauthorized exposure of sensitive information. The agency also would be required to disclose a suspected breach of or unauthorized exposure of information to those affected as soon as possible.

Vendor responsibility for cybersecurity. A vendor that provided information resources technology or services for a state agency would be responsible for providing contracting personnel with written acknowledgement of any known cybersecurity risks identified in vulnerability and penetration testing of an agency's website or mobile application and a strategy for and costs associated with mitigating them. A vendor also would have to prove that any individual servicing the contract held certain industry-recognized certifications.

Purchase of cloud computing services. DIR would be required to periodically review guidelines on state agency information that could be stored by a cloud computing or other storage service to ensure that an agency selected the most affordable, secure, and efficient storage service. The guidelines would have to include privacy and security standards that required a vendor who offered storage or other IT-related services to demonstrate that the agency's data would be maintained in compliance with state and federal laws.

Security issues related to legacy systems. A state agency would have to include in a plan to mitigate information security issues related to legacy, or outdated, systems a strategy for mitigating any workforce-related discrepancy in cyber-related positions with the appropriate training and certifications, among other information specified in the bill.

Continuing education and industry-recognized certifications. CSHB 8 would require DIR to provide mandatory guidelines to state agencies regarding continuing education requirements for cybersecurity training and the industry-recognized certifications that would be completed by all information resources employees. A state agency could spend public funds to reimburse fees associated with certification examinations to an employee who served in a cyber-related position.

Study on digital data storage and records management. The DIR and the Texas State Library and Archives Commission would be required to conduct a study that examined state agency digital data storage and records management practices and the associated costs. The agencies would submit a report on the study to the lieutenant governor, the House speaker, and the legislative committees with appropriate jurisdiction by December 1, 2018.

Election cyberattack study. The bill would require the secretary of state to conduct a study regarding cyberattacks on election infrastructure that included an investigation of vulnerabilities and risks for a cyberattack against voting machines or the list of registered voters, information on any attempted attack, and recommendations for protecting voting machines and the list of voters. The secretary could contract with a qualified vendor to conduct the study. A copy of a public summary and a confidential report would have to be submitted to the legislative committees with appropriate jurisdiction by December 1, 2018.

Select committees on cybersecurity. The bill would require the lieutenant governor and the House speaker each to establish a five-member select committee to study cybersecurity in Texas, the information security plans of each agency, and the risks and vulnerabilities of state agency cybersecurity by November 30, 2017. The committees would jointly report to the Legislature any findings and recommendations by January 13, 2019.

Sunset review process. The bill would require the Sunset Advisory

Commission to consider an assessment of an agency's cybersecurity practices during the Sunset review process. In this assessment, the commission could use available information from DIR or any other state agency.

Effective date. The bill would take effect September 1, 2017, and would not apply to the Electric Reliability Council of Texas.

SUPPORTERS SAY:

CSHB 8 would reduce Texas' vulnerability to cyberattacks by assessing risk at state agencies, increasing efforts to protect sensitive and confidential data, closing the workforce skills gap, and ensuring that agencies have incident response plans. As the world becomes more reliant on digitally-connected infrastructure, cyber-related incidents can affect the economy, the government, and the lives of private citizens. Texas currently is behind other states in enacting cybersecurity initiatives. Therefore, it is critical to ensure agencies have the necessary tools to protect the state from the evolving world of sophisticated cyberattacks.

Investing in the state's cyber infrastructure and personnel would help to prevent serious losses of sensitive data, potentially saving millions of dollars in recovery services in the future. A significant state data breach could cost the state money and public trust. While there would be initial costs to implement the bill, these should decrease over time because the cost of maintaining the infrastructure would not be as significant as updating it.

Continuing education and industry-recognized certifications. The human factor is the most important component to cybersecurity. Agencies can expend resources on infrastructure, but if cyber-related personnel lack skills and training, the agency remains vulnerable. Also, workforce demand is high in cyber-related positions. The bill would prioritize workforce development and closing the IT skills gap to help the state build a more confident, skilled workforce by adding routine cyberhygiene training for state agency personnel and requiring continuing education for cyber-related personnel.

Independent risk assessment. Risk assessments are critical for proactively addressing security concerns. The bill would require the assessments to be conducted by a third party to ensure that a biased perspective did not sway the results. Allowing agencies to select from a list of vendors already approved by DIR would eliminate the burden on agencies to find their own vendors and could lead to economies of scale on state purchases while also standardizing the quality of the assessments.

Data security procedures for online and mobile applications. Requiring DIR to advise an agency in the development stage of a website or application would be a positive step for reducing vulnerabilities early in the process. The bill would provide measures to alleviate a potential burden on DIR by allowing a state agency with a security plan previously approved by DIR to review subsequent plans internally, if the agency also had the sufficient personnel and technology to do so.

Individual identifying information. By requiring agencies to regularly destroy personally identifiable information, the bill would greatly reduce the chances of it being stolen. Spending thousands of dollars to destroy unnecessarily stored information could save agencies millions of dollars in the event of a breach. The bill also would give an agency two years from the effective date to comply, providing ample time for an agency to separate data if needed and to create policies on data storage.

Vendor responsibility for cybersecurity. The bill would ensure that the executive head of an agency retained full responsibility for the agency's information security and any associated risks.

Security breach notification. The bill would standardize reporting for when it was suspected that sensitive data had been compromised. It is important to require all agencies to be in the practice of notification so that DIR would be aware of each actual and suspected incident that occurred.

OPPONENTS SAY:

CSHB 8 would create additional burdens on state agencies that already are overwhelmed and underfunded. DIR already performs some of the functions required by the bill, creating an element of redundancy.

Independent risk assessment. The bill would require agencies to perform an independent risk assessment at least once every five years. By requiring the risk assessment to be performed by a third party, the bill would result in significant costs to agencies and to DIR.

Data security procedures for online and mobile applications. Currently, agencies control their websites and mobile applications, and DIR becomes involved only upon request. The bill would require DIR to review websites and applications during development, which could be burdensome and result in the department needing to seek out vendors and enter into new costly contracts to comply.

Individual identifying information. It could be costly for agencies to destroy or arrange for the destruction of personally identifiable information. Some agencies do not separate data they collect based on its sensitivity. Thus, in addition to the costs for destruction, agencies would have to expend both time and money separating data.

Vendor responsibility for cybersecurity. The bill would require a vendor that provided cyber-related services for a state agency to submit written acknowledgement of any known cybersecurity risks identified in vulnerability and penetration testing and a strategy for them. However, because it appears the bill would not require agencies to address any discovered vulnerability, it is unclear whether the vendor or the agency would be liable in the event of a breach.

Security breach notification. The bill would require entities to notify the public not only in the event of a breach or suspected breach but also when an unauthorized exposure of information was discovered. An unauthorized exposure of information may not involve confidential information or result in a risk to the public. Requiring notification in these cases could be costly and burdensome for agencies.

OTHER OPPONENTS

CSHB 8 would be a necessary step for the state to take in creating a holistic approach to cybersecurity. However, if the bill's mandates went

SAY:

unfunded and agencies were not given the resources to comply, the state would be no less vulnerable than it already is.

NOTES:

Fiscal note. According to the Legislative Budget Board, the statewide fiscal implications could not be determined because the impact would be contingent on certain factors, such as an agency's existing IT infrastructure, current practices, and the number of full-time equivalent (FTE) positions currently supporting cyber-related functions. The LBB estimates that some agencies could incur significant costs. The cumulative impact to the Department of Public Safety would be estimated to be a cost of $6.1 million in general revenue funds, including three additional FTEs. Other costs to agencies could involve conducting independent risk assessments, performing vulnerability and penetration tests, and destroying information.

Comparison to bill as filed. CSHB 8 differs from the bill as filed in several ways, including that the committee substitute would:

- authorize fee reimbursements to certain entities for appropriate industry-recognized certification examinations;
- allowing all governmental bodies to discuss cybersecurity related issues in a closed meeting;
- requiring the cybersecurity task force to address workforce gaps;
- adding in a state agency's information security plan that vendors would have to comply with applicable state and federal law;
- requiring that only high priority vulnerabilities, rather than all vulnerabilities, be identified before deploying a website;
- requiring written acknowledgement to be submitted by a vendor to a state agency;
- not requiring destruction of records kept for law enforcement purposes;
- requiring the secretary of state to study election cyberattacks, rather than the Texas Rangers; and
- other changes to reflect federal standards and current state agency practices.