BILL ANALYSIS

Senate Research Center

H.B. 8
By: Capriglione et al. (Nelson)
Business & Commerce
5/13/2017
Engrossed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Interested parties contend that, as sensitive information is increasingly stored online, there must be a commensurate increase in efforts to protect the data of private citizens from rapidly evolving and sophisticated cyber-attacks. H.B. 8 seeks to minimize Texas' vulnerability to cyber attacks by creating an Information and Analysis Center, providing guidelines for cybersecurity training, requiring risk assessments, and providing other best practice guidance.

H.B. 8 amends current law relating to cybersecurity for state agency information resources.

RULEMAKING AUTHORITY

This bill does not expressly grant any additional rulemaking authority to a state officer, institution, or agency.

SECTION BY SECTION ANALYSIS

SECTION 1. Authorizes this Act to be cited as the Texas Cybersecurity Act.

SECTION 2. Amends Section 325.011, Government Code, as follows:

> Sec. 325.011. CRITERIA FOR REVIEW. Requires the Sunset Advisory Commission and its staff to consider certain criteria in determining whether a public need exists for the continuation of a state agency or its advisory committees or for the performance of the functions of the agency or its advisory committees, including an assessment of the agency's cybersecurity practices using information available from the Texas Department of Information Resources (DIR) or any other appropriate state agency. Makes a nonsubstantive change.

SECTION 3. Amends Subchapter B, Chapter 421, Government Code, by adding Section 421.027, as follows:

> Sec. 421.027. CYBER INCIDENT STUDY AND RESPONSE PLAN. (a) Defines "cyber incident" and "significant cyber incident."
>
>> (b) Requires the Homeland Security Council (council), in cooperation with DIR, to conduct a study regarding cyber incidents and significant cyber incidents affecting state agencies and critical infrastructure that is owned, operated, or controlled by agencies; and develop a comprehensive state response plan to provide a format for each state agency to develop an agency-specific response plan and to implement the plan into the agency's information security plan required under Section 2054.133 (Information Security Plan) to be implemented by the agency in the event of a cyber-incident or significant cyber incident affecting the agency or critical infrastructure that is owned, operated, or controlled by the agency.
>>
>> (c) Requires the council, not later than September 1, 2018, to deliver the response plan and a report on the findings of the study to certain individuals.

(d) Provides that the response plan required by Subsection (b) and the report required by Subsection (c) are not public information for purposes of Chapter 552 (Public Information).

(e) Provides that this section expires December 1, 2018.

SECTION 4. Amends Section 551.089, Government Code, as follows:

Sec. 551.089. New heading: DELIBERATION REGARDING SECURITY DEVICES OR SECURITY AUDITS; CLOSED MEETING. Provides that this chapter (Open Meetings) does not require a governmental body, rather than the governing board of DIR, to conduct an open meeting to make certain deliberations.

SECTION 5. Amends Section 552.139, Government Code, by adding Subsection (d), as follows:

(d) Requires a state agency, when posting a contract on an Internet website as required by Section 2261.253 (Required Posting of Certain Contracts; Enhanced Contract and Performance Monitoring), to redact information made confidential by this section (Exception: Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers) or excepted from public disclosure by this section. Provides that a redaction under this subsection does not except information from the requirements of Section 552.021 (Availability of Public Information).

SECTION 6. Amends the heading to Section 656.047, Government Code, to read as follows:

Sec. 656.047. PAYMENT OF PROGRAM AND CERTIFICATION EXAMINATION EXPENSES.

SECTION 7. Amends Section 656.047, Government Code, by adding Subsection (a-1), to authorize a state agency to spend public funds as appropriate to reimburse a state agency employee or administrator who serves in an information technology, cybersecurity, or other cyber-related position for fees associated with industry-recognized certification examinations.

SECTION 8. Amends Subchapter C, Chapter 2054, Government Code, by adding Section 2054.0594, as follows:

Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS CENTER. (a) Requires DIR to establish an information sharing and analysis center to provide a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies.

(b) Requires DIR to appoint persons from appropriate state agencies to serve as representatives to the information sharing and analysis center.

(c) Requires DIR, using existing resources, to provide administrative support to the information sharing and analysis center.

SECTION 9. Amends Section 2054.076, Government Code, by adding Subsection (b-1), as follows:

(b-1) Requires DIR to provide mandatory guidelines to state agencies regarding the continuing education requirements for cybersecurity training and the industry-recognized certifications that are required to be completed by all information resources employees of the agencies. Requires DIR to consult with the Information Technology Council for Higher Education (ITCHE) on applying the guidelines to institutions of higher education (IHEs).

SECTION 10. Amends Sections 2054.077(b) and (e), Government Code, as follows:

(b) Requires, rather than authorizes, the information resources manager of a state agency to prepare or have prepared a certain report relating to the vulnerability of certain electronic equipment of the agency.

(e) Requires a state agency, separate from the executive summary described by Subsection (b), to prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. Deletes existing text specifying a state agency whose information resources manager has prepared or has had prepared a vulnerability report is required to provide a certain summary.

SECTION 11. Amends Section 2054.1125(b), Government Code, as follows:

(b) Requires a state agency that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law to, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

(1) comply with the notification requirements of Section 521.053 (Notification Required Following Breach of Security of Computerized Data), Business & Commerce Code, to the same extent as a person who conducts business in this state; and

(2) not later than 48 hours after the discovery of the breach, suspected breach, or unauthorized exposure, notify DIR, including the chief information security officer and the state cybersecurity coordinator or, if the breach, suspected breach, or unauthorized exposure involves election data, the secretary of state (SOS).

Makes a conforming change.

SECTION 12. Amends Section 2054.133, Government Code, by adding Subsections (b-1), (b-2), (b-3), and (b-4), as follows:

(b-1) Requires the executive head and chief information security officer of each state agency to annually review and approve in writing the agency's information security plan and strategies for addressing the agency's information resources systems that are at highest risk for security breaches. Requires that the plan at a minimum include solutions that isolate and segment sensitive information and maintain architecturally sound and secured separation among networks. Requires the highest ranking information security employee for the agency, if a state agency does not have a chief information security officer, to review and approve the plan and strategies. Provides that the executive head retains full responsibility for the agency's information security and any risks to that security.

(b-2) Requires a state agency, before submitting to the Legislative Budget Board (LBB) a legislative appropriation request for a state fiscal biennium, to file with LBB the written approval required under Subsection (b-1) for each year of the current state fiscal biennium.

(b-3) Requires each state agency to include in the agency's information security plan the actions the agency is taking to incorporate into the plan the core functions of "identify, protect, detect, respond, and recover" as recommended in the "Framework for Improving Critical Infrastructure Cybersecurity" of the United States Department of Commerce National Institute of Standards and Technology. Requires the agency to, at a minimum, identify any information the agency requires individuals to provide to the agency or the agency retains that is not necessary for the agency's operations. Authorizes the agency to incorporate the core functions over a period of years.

(b-4) Requires a state agency's information security plan to include appropriate privacy and security standards that, at a minimum, require a vendor who offers cloud computing services or other software, applications, online services, or information technology solutions to any state agency to contractually warrant that data provided by the state to the vendor will be maintained in compliance with all applicable state and federal laws and rules.

SECTION 13. Amends Section 2054.512, Government Code, as follows:

Sec. 2054.512. New heading: CYBERSECURITY COUNCIL. (a) Requires, rather than authorizes, the state cybersecurity coordinator to establish and lead a cybersecurity council includes public and private sector leaders and cybersecurity practitioners to collaborate on matters of cybersecurity concerning this state. Creates this subsection from existing text.

(b) Requires the cybersecurity council to include certain members.

(c) Requires the state cybersecurity coordinator, in appointing representatives from IHEs to the cybersecurity council, to consider appointing members of ITCHE.

(d) Requires the cybersecurity council to provide recommendations to the legislature on any legislation necessary to implement cybersecurity best practices and remediation strategies for this state.

SECTION 14. Amends Subchapter N-1, Chapter 2054, Government Code, by adding Sections 2054.515, 2054.516, 2054.517, 2054.518, and 2054.519, as follows:

Sec. 2054.515. INDEPENDENT RISK ASSESSMENT. (a) Requires each state agency, at least once every five years, in accordance with DIR rules, to:

(1) contract with an independent third party selected from a list provided by DIR to conduct an independent risk assessment of the agency's exposure to security risks in the agency's information resources systems and to conduct tests to practice securing systems and notifying all affected parties in the event of a data breach; and

(2) submit the results of the independent risk assessment to DIR.

(b) Requires DIR to annually compile the results of the independent risk assessments conducted in the preceding year and prepare certain reports.

(c) Requires DIR to annually submit to the legislature a comprehensive report on the results of the independent risk assessments conducted under Subsection (a) during the preceding year that includes a certain report and that identifies systematic or pervasive security risk vulnerabilities across state agencies and recommendations for addressing the vulnerabilities but does not contain any information the release of which may compromise any state agency's information resources system.

Sec. 2054.516. DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS. (a) Requires each state agency, other than an IHE subject to Section 2054.517, implementing an Internet website or mobile application that processes any personally identifiable or confidential information to:

(1) submit a data security plan to DIR during development and as early as feasible in the testing of the website or application and submit any modification to the plan made during development; and

(2) before deploying the website or application:

(A) subject the website or application to a vulnerability and penetration test conducted by an independent third party; and

(B) address any high priority vulnerability identified under Paragraph (A).

(b) Requires the data security plan required under Subsection (a)(1) to include certain information, diagrams, descriptions, and standards.

(c) Requires DIR, unless a state agency has previously submitted a comprehensive security plan approved by DIR and has sufficient personnel and technology to review plans internally, to review each data security plan submitted under Subsection (a) and make any recommendations for changes to the plan to the state agency as soon as practicable after DIR reviews the plan.

(d) Provides that a data security plan submitted under Subsection (a) and any recommendation for changes made under Subsection (c) are not public information for purposes of Chapter 552.

Sec. 2054.517. DATA SECURITY PROCEDURES FOR ONLINE AND MOBILE APPLICATIONS OF INSTITUTIONS OF HIGHER EDUCATION. (a) Requires each IHE, as defined by Section 61.003 (Definitions), Education Code, to adopt and implement a policy for Internet website and mobile application security procedures that complies with this section.

(b) Requires the developer of the website or application for the IHE, before deploying an Internet website or mobile application that processes confidential information for an IHE, to submit to the IHE's information security officer the information required under policies adopted by the IHE to protect the privacy of individuals by preserving the confidentiality of information processed by the website or application. Requires the IHE's policies, at a minimum, to require the developer to submit information describing the architecture of the website or application, the authentication mechanism for the website or application, and the administrator level access to data included in the website or application.

(c) Requires an IHE, before deploying an Internet website or mobile application described by Subsection (b), to subject the website or application to a vulnerability and penetration test conducted internally or by an independent third party.

(d) Requires each IHE to submit to DIR the policies adopted as required by Subsection (b). Requires DIR to review the policies and make recommendations for appropriate changes.

Sec. 2054.518. VENDOR RESPONSIBILITY FOR CYBERSECURITY. Provides that a vendor that contracts with this state to provide information resources technology for a state agency at a cost to the agency of $1 million or more is responsible for addressing known cybersecurity risks associated with the technology and is responsible for any cost associated with addressing the identified cybersecurity risks. Requires the vendor, for a major information resources project, to provide to state agency contracting personnel:

(1) written acknowledgment of any known cybersecurity risks associated with the technology identified in the vulnerability and penetration test conducted under Section 2054.516 or Section 2054.517;

(2) proof that any individual servicing the contract holds the appropriate industry-recognized certifications as identified by the National Initiative for Cybersecurity Education;

(3) a strategy for mitigating any technology or personnel-related cybersecurity risk identified in the vulnerability and penetration test conducted under Section 2054.516 or Section 2054.517; and

(4) an initial summary of any costs associated with addressing or remediating the identified technology or personnel-related cybersecurity risks as identified in collaboration with this state following a risk assessment.

Sec. 2054.519. CYBERSECURITY RISKS AND INCIDENTS. (a) Requires DIR to develop a plan to address cybersecurity risks and incidents in this state. Authorizes DIR to enter into an agreement with a national organization, including the National Cybersecurity Preparedness Consortium, to support DIR's efforts in implementing the components of the plan for which DIR lacks resources to address internally. Authorizes the agreement to include certain provisions.

(b) Requires DIR, in implementing the provisions of the agreement prescribed by Subsection (a), to seek to prevent unnecessary duplication of existing programs or efforts of DIR or another state agency.

(c) Requires DIR, in selecting an organization under Subsection (a), to consider the organization's previous experience in conducting cybersecurity training and exercises for state agencies and political subdivisions.

(d) Requires DIR to consult with IHEs in this state when appropriate based on an IHE's expertise in addressing specific cybersecurity risks and incidents.

SECTION 15. Amends Section 2054.575(a), Government Code, as follows:

(a) Requires a state agency to, with available funds, identify information security issues and develop a plan to prioritize the remediation and mitigation of those issues. Requires the agency to include in the plan certain procedures, approaches, analyses, information, and strategies.

SECTION 16. Amends Section 2059.055(b), Government Code, to change a reference to a state agency to a governmental entity.

SECTION 17. Amends Subtitle B, Title 10, Government Code, by adding Chapter 2061, as follows:

CHAPTER 2061. INDIVIDUAL-IDENTIFYING INFORMATION

Sec. 2061.001. DEFINITIONS. Defines "cybersecurity risk" and "state agency."

Sec. 2061.002. DESTRUCTION AUTHORIZED. (a) Requires a state agency to destroy or arrange for the destruction of information that presents a cybersecurity risk and alone or in conjunction with other information identifies an individual in connection with the agency's networks, computers, software, or data storage if the agency is otherwise prohibited by law from retaining the information for a period of years.

(b) Requires a state agency to destroy or arrange for the destruction of information described by Subsection (a) in accordance with standards for destruction of data prescribed in the National Security Program Operating Manual, 1995 edition.

(c) Provides that this section does not apply to a record involving criminal activity or a criminal investigation retained for law enforcement purposes.

(d) Prohibits a state agency from destroying or arranging for the destruction of any election data before the third anniversary of the date the election to which the data pertains is held.

(e) Prohibits a state agency, under any circumstance, from selling certain information.

(f) Requires each state agency, not later than September 1, 2019, to develop the systems and policies necessary to comply with this section. Provides that this subsection expires September 1, 2020.

SECTION 18. Amends Section 2157.007, Government Code, by adding Subsection (e), as follows:

(e) Requires DIR to periodically review guidelines on state agency information that is authorized to be stored by a cloud computing or other storage service and the cloud computing or other storage services available to state agencies for that storage to ensure that an agency purchasing a major information resources project under Section 2054.118 (Major Information Resources Project) selects the most affordable, secure, and efficient cloud computing or other storage service available to the agency. Requires that the guidelines include appropriate privacy and security standards that, at a minimum, require a vendor who offers cloud computing or other storage services or other software, applications, online services, or information technology solutions to any state agency to demonstrate that data provided by the state to the vendor will be maintained in compliance with all applicable state and federal laws and rules.

SECTION 19. Amends Chapter 276, Election Code, by adding Section 276.011, as follows:

Sec. 276.011. ELECTION CYBER ATTACK STUDY. (a) Requires SOS, not later than December 1, 2018, to:

(1) conduct a study regarding cyber attacks on election infrastructure;

(2) prepare a public summary report on the study's findings that does not contain any information the release of which may compromise any election;

(3) prepare a confidential report on specific findings and vulnerabilities that is exempt from disclosure under Chapter 552, Government Code; and

(4) submit a copy of the report required under Subdivision (2) and a general compilation of the report required under Subdivision (3) that does not contain any information the release of which may compromise any election to the standing committees of the legislature with jurisdiction over election procedures.

(b) Requires that the study include:

(1) an investigation of vulnerabilities and risks for a cyber-attack against a county's voting system machines or the list of registered voters;

(2) information on any attempted cyber attack on a county's voting system machines or the list of registered voters; and

(3) recommendations for protecting a county's voting system machines and list of registered voters from a cyber-attack.

(c) Authorizes SOS, using existing resources, to contract with a qualified vendor to conduct the study required by this section.

(d) Provides that this section expires January 1, 2019.

SECTION 20. (a) Requires the lieutenant governor to establish a Senate Select Committee on Cybersecurity and the speaker of the house of representatives to establish a House Select Committee on Cybersecurity to, jointly or separately, study cybersecurity in this state, the information security plans of each state agency, and the risks and vulnerabilities of state agency cybersecurity.

(b) Requires, not later than November 30, 2017, the lieutenant governor to appoint five senators to the Senate Select Committee on Cybersecurity, one of whom is required to be designated as chair, and the speaker of the house of representatives to appoint five state representatives to the House Select Committee on Cybersecurity, one of whom is required to be designated as chair.

(c) Requires that the committees established under this section convene separately at the call of the chair of the respective committees, or jointly at the call of both chairs. Requires the chairs of each committee, in joint meetings, to act as joint chairs.

(d) Requires the committees established under this section, following consideration of the issues listed in Subsection (a) of this section, to jointly adopt recommendations on state cybersecurity and report in writing to the legislature any findings and adopted recommendations not later than January 13, 2019.

(e) Provides that this section expires September 1, 2019.

SECTION 21. (a) Defines "state agency."

(b) Requires DIR and the Texas State Library and Archives Commission (TSLAC) to conduct a study on state agency digital data storage and records management practices and the associated costs to this state.

(c) Requires that the study required under this section examine certain practices, costs, policies, solutions, and benefits.

(d) Requires each state agency to participate in the study required by this section and provide appropriate assistance and information to DIR and TSLAC.

(e) Requires DIR and TSLAC, not later than December 1, 2018, to issue a report on the study required under this section and recommendations for reducing state costs and for improving efficiency in digital data storage and records management to the lieutenant governor, the speaker of the house of representatives, and the appropriate standing committees of the house of representatives and the senate.

(f) Provides that this section expires September 1, 2019.

SECTION 22. Provides that the changes in law made by this Act do not apply to the Electric Reliability Council of Texas.

SECTION 23. Effective date: September 1, 2017.