SUBJECT: Creating programs, requirements for agencies to assess cybersecurity risk

COMMITTEE: State Affairs — committee substitute recommended

VOTE: 11 ayes — Phelan, Hernandez, Guerra, Harless, Hunter, P. King, Parker, Raymond, E. Rodriguez, Smithee, Springer

0 nays

2 absent — Deshotel, Holland

WITNESSES: For — (*Registered, but did not testify*: Russell Mullins, Alterity Solutions, Inc.; Jim Keffer, City of Del Rio; James Dickey, Republican Party of Texas; Justin Yancy, Texas Business Leadership Council; Nora Belcher, Texas e-Health Alliance; Joe Buser, Traveling Coaches, Inc.; Idona Griffith; Russell Hayter)

Against — None

BACKGROUND: It has been suggested that smaller state agencies and local governmental entities could use additional support to help decrease cybersecurity risk.

DIGEST: CSHB 4214 would create programs and requirements for state agencies and local governments to assess cybersecurity risks.

Regional ISACs. The state cybersecurity coordinator would provide for the establishment and operation of up to 20 regional information sharing and analysis centers (ISAC) located throughout the state. The boundaries for each center would be coextensive with regional education service centers established under state law.

Each municipality with a population of more than 25,000 would have to join the regional ISAC in which it was predominantly located, and any other political subdivision could join an ISAC in which it was predominantly located.

Notifications. A political subdivision would have to notify the regional ISAC within 48 hours of the discovery of a breach or suspected breach of system security or an unauthorized exposure of sensitive information. The ISAC would report the breach to the Department of Information Resources (DIR) if the person responsible obtained or modified personal information, accessed information systems or infrastructure, or disrupted a core function.

A political subdivision would have to notify the cybersecurity coordinator within 48 hours of making a ransomware payment.

A local government that owned, licensed, or maintained data that included sensitive personal information would have to comply with these notification requirements.

Multihazard plan, security audit. Each municipality or county with a population of more than 100,000 would have to implement a multihazard emergency operations plan that addressed mitigation, preparedness, response, and recovery. The plan would have to provide for employee training in emergency response, coordination with state and local entities in the event of an emergency, and a safety and security audit.

At least once every three years, each municipality and county would have to conduct a safety and security audit of information technology infrastructure and report the results to the municipality's or county's governing body and the cybersecurity council.

Information related to the audit would not be subject to public information laws. A document related to the emergency plan would be subject to disclosure if it enabled a person to verify certain information as specified in the bill.

Definition of disaster. The bill would add cyber attack to the list of occurrences or imminent threats that were considered a disaster for the purposes of the Texas Disaster Act.

Continuous monitoring program. Each state agency would be required to develop and maintain an information security continuous monitoring program that satisfied certain requirements listed in the bill, including maintaining ongoing awareness of the vulnerabilities of and threats to the information resources, setting priorities to manage organizational risk, and addressing critical security controls. The program would have to align with guidance from the U.S. Department of Commerce's National Institute of Standards and Technology.

DIR would be required to assist each state agency in implementing a continuous monitoring program and establish a statewide dashboard that provided a government-wide view of monitoring and technical guidance.

Risk assessments. At least once every five years, each state agency would have to contract with an independent third party to conduct a risk assessment of information resources systems and practice securing systems and notifying all affected parties in the event of a data breach.

DIR annually would have to compile the results of assessments conducted in the previous year and prepare both a public report on general security issues that did not contain any sensitive information and a confidential report on specific risks and vulnerabilities that would be exempt from public information laws.

The bill would require DIR to submit to the Legislature annually the results of the assessments during the preceding year, including the public report, and provide recommendations to address pervasive security risk vulnerabilities across state agencies. This report could not contain any sensitive information.

DIR would have to develop a cybersecurity threat assessment for local governments that provided best practices for preventing cyber attacks.

Each school district or public junior college district would have to conduct a cybersecurity assessment at least once every three years.

Cyber incident study and response plan. The state Homeland Security Council, in cooperation with DIR, would be required to study cyber incidents and significant cyber incidents affecting state agencies and critical infrastructure owned, operated, or controlled by agencies.

The council would have to develop a comprehensive state response plan as a format for agency-specific plans. Each state agency would implement the plan into its information security plan required under law for use in the event of an incident affecting the agency or critical infrastructure.

By September 1, 2020, the council would have to deliver the response plan and a report on the study's findings to the public safety director of the Department of Public Safety, the governor, the lieutenant governor, the House speaker, and legislative committees with appropriate jurisdiction.

The response plan and report would not be public information for the purposes of state open records laws, and related provisions would expire December 1, 2020.

Cyber operations. The governor could command the Texas National Guard to assist the Texas State Guard with defending the state's cyber operations.

Cybersecurity threat simulation exercises. Executive staff of a state agency could participate in cybersecurity threat simulation exercises with the agency's information resources technologies employees to test cybersecurity capabilities.

Chief innovation officer. CSHB 4214 would require the governor to appoint a chief innovation officer to improve internal state government efficiency and performance, develop methods to improve interaction with state government, work with DIR to increase the use of technology by state agencies, and provide training in skills to support innovation and encourage creative thinking.

Security program for certain objects. DIR would be required to develop

a comprehensive risk management program that identified baseline security features for the internet connectivity of computing devices embedded in objects used or purchased by state agencies.

To develop the program, DIR would consult with industry representatives, voluntary standards organizations, and the 10 state agencies that received the most state appropriations for that fiscal year. DIR would have to study and report to the Legislature on these types of objects by December 31, 2020.

A vendor offering to sell one of these objects would have to include with each bid, offer, or proposal a written certification providing that the good did not contain a hardware, software, or firmware component with any known security vulnerability or defect.

Vendor responsibility for cybersecurity. A vendor that provided a state agency technology at a cost of $1 million or more would be responsible for addressing known cybersecurity risks and for any associated costs.

For a major information resources project, the vendor would have to provide a written attestation to agency contracting personnel that it had a cybersecurity risk management program consistent with accepted security management frameworks, that the program included appropriate training and certifications for employees, and that the vendor had a vulnerability management program that addressed identification, mitigation, and responsible disclosure, as appropriate.

The vendor also would have to provide an initial summary of any costs associated with addressing technology or personnel-related cybersecurity risks identified in collaboration with the state following a risk assessment.

Encrypted secure layer services. The bill would require each state agency that maintained a publicly accessible website that required the submission of sensitive personally identifiable information to use an encrypted secure communication protocol.

Liability exemption. A person who, in good faith, disclosed to a governmental entity information regarding a potential security issue would not be liable for any civil damages resulting from the disclosure unless the person stole, retained, or sold any data obtained as a result of the security issue.

Next generation technology. Each state agency and local government would be required to consider using next-generation technologies, including cryptocurrency, blockchain technology, and artificial intelligence.

Cloud computing service. Rather than requiring a state agency to consider cloud computing service options when purchasing a major information resources project, the bill would require a state agency to ensure that an automated information system or major project was capable of being deployed and run on cloud computing services.

DIR periodically would have to review guidelines on state agency information that could be stored by a cloud computing or other service and the available services to ensure that an agency purchasing a major information resources project selected the most affordable, secure, and efficient storage service.

The guidelines would include appropriate privacy and security standards that, at a minimum, required a vendor who offered storage services or other information technology solutions to demonstrate that data provided by the state to the vendor would be maintained in compliance with all applicable state and federal laws and rules.

Cybersecurity training for new employees. DIR would have to develop and provide training for new state agency employees on cybersecurity measures and awareness, which employees would have to complete within 30 days of their hiring date.

Cyberstar program. The state cybersecurity coordinator would be required to establish a cyberstar certificate program to recognize public

and private entities that implemented best practices for cybersecurity. It would be developed by the coordinator in collaboration with the cybersecurity council and public and private entities. The program would have to allow DIR to issue a certificate of approval to an entity that complied with the best practices, and the entity could include the certificate in advertisements and other public communications.

The cybersecurity coordinator would have to conduct an annual public event promoting best practices for cybersecurity as listed in the bill.

Payment of program expenses. The bill would allow a state agency to spend public funds to reimburse an employee who served in a cyber-related position for fees associated with industry-recognized certification exams.

Cybersecurity certificate programs. The bill would require the Texas Higher Education Coordinating Board, in consultation with DIR, to coordinate with lower-division institutions of higher education and other entities to develop cybersecurity certificate or credential programs or other courses of instruction leading toward such credentials that could be offered by the lower-division institutions of higher education.

Repository for cybersecurity education, training. DIR, in conjunction with institutions of higher education, would have to maintain and promote a centralized repository of information on cybersecurity education and training that was available to any governmental entity in the state.

Middle, high school access. The bill would expand the responsibilities of the state cybersecurity council to include ensuring all middle and high schools had knowledge of and access to free cybersecurity courses and curriculum approved by the Texas Education Agency, state and regional ISACs, and certain contracting benefits under law.

Matching grants. Using available funds, the governor would be required to administer a cybersecurity matching grant program for local governmental entities to defray the costs of cybersecurity projects.

A local governmental entity that applied for a grant would have to identify the source and amount of matching funds. If the application was approved, the Office of the Governor would have to award a grant equal to 150 percent of the amount committed by the entity.

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, the information security plans of each agency, the risks and vulnerabilities of state agency cybersecurity, and information technology procurement by November 30, 2019. The committees would jointly report any findings and recommendations to the Legislature by January 12, 2021.

The bill would take effect September 1, 2019.

NOTES: According to the Legislative Budget Board, the cost associated with the bill could be significant. Although indeterminate, the minimum costs associated with the bill would be $3.8 million in general revenue through fiscal 2020-21.