Leadership Role

New laws are putting Texas at the forefront in addressing cybersecurity as a matter of public policy.

BY ELIZABETH ROGERS

The 85th Texas Legislature considered and approved a variety of cybersecurity-related legislation during the regular session that went into effect a little over a year ago on September 1, 2017. From a substantive perspective, versus a numeric one, Texas has taken a leadership role in addressing various public sector cybersecurity and data privacy issues.

Texas laws cover a range of relevant concerns, such as required practices for state agencies, continuous monitoring and auditing of network systems and processes, updating the penal code for the digital era, and important student data privacy protections. Other states have taken steps to address some of these issues but the newly adopted Texas legislative approach is comprehensive.

House Bill 8—Texas Cybersecurity Act

The Texas Cybersecurity Act establishes certain cybersecurity requirements for all state agencies in Texas, adds cybersecurity as an element of the Sunset review process, creates a cybersecurity council, and requires that certain agencies conduct studies and reports related to cybersecurity threats and responses. Texas House Speaker Joe Straus commented that the overarching goal of HB 8 is "to ensure state agencies are good stewards of private data."[1]

Consideration of Cybersecurity in Sunset Review Process. The Sunset Advisory Commission, an agency of the Texas Legislature, evaluates whether state agencies should be reformed, continued, or abolished, and makes recommendations to the Legislature to that effect. When determining whether a public need exists for the continuation of a state agency, the commission is now required to assess the agency's cybersecurity practices using information provided by the Department of Information Resources, or DIR, or any other appropriate state agency.[2]

Expanding the Role of the Texas DIR. HB 8 requires the DIR to develop and implement a plan to address cybersecurity risks and incidents in the state and authorized the agency to enter into an agreement, as needed, with an organization such as the National Cybersecurity Preparedness Consortium to support implementation efforts.[3] Earlier this year, the DIR worked with the Statewide Information Security Advisory Committee to create a statewide strategic five-year plan, with five goals.[4]

As part of the requirements of HB 8, the DIR will establish an "information sharing and analysis center," or ISAC, in the fourth quarter of 2018, "to provide a forum for agencies to share information regarding cybersecurity threats, best practices, and remediation strategies."[5] And, mandatory guidelines and requirements are in progress for the cybersecurity training to be completed by all state agency information resources employees[6] and the biennial information security assessment and report that all state agencies must now conduct (discussed further below).[7]

Changes for State Agencies. Prior to passage of HB 8, state agencies were required to identify information security issues and develop a plan to prioritize the remediation and mitigation of those issues. This legislation adds specificity to that requirement by delineating five specific elements that an agency must consider when identifying the issues and developing the plan.[8,9]

Each state agency is now required to conduct an information security assessment of the agency's network systems, data storage systems, data security measures, and information resources vulnerabilities at least once every two years and to report the results to the DIR.[10] Similarly, each state agency shall submit a biennial data security plan to the DIR and conduct a vulnerability and penetration test of the agency's website and any mobile applications that process any personally identifiable or confidential information.[11]

Colleges and Universities. Institutions of higher education must adopt and implement a policy for websites or mobile applications operated by the institution to ensure that the privacy of individuals is protected and the confidentiality of information processed by the websites or applications is preserved.[12]

Open Meetings Act. The Texas Cybersecurity Act makes key changes to the state's Open Meetings Act. All governmental bodies in Texas are now permitted to conduct closed meetings to deliberate network security assessments or deployments of security personnel, infrastructure, or devices.[13] This new exception offers the freedom that an entity needs to properly deliberate these sensitive matters. Yet, any entity utilizing this provision must be careful to limit such deliberations to the appropriate topic so as to not violate separate provisions of the Open Meetings Act.

Data Breaches. With respect to data breaches, HB 8 expands the categories of information that, if compromised, would trigger an agency's duty to notify affected individuals.[14] HB 8 also adds an additional requirement that state agencies must now report a data breach or suspected data breach of system security to the DIR.[15]

Another provision of the bill requires the Texas secretary of state to conduct a study regarding cyberattacks on election infrastructure. The study must include an investigation of vulnerabilities in election infrastructure, information on any attempted cyberattack on a county's voting machines or registered voter lists, and recommendations for protecting voting machines and voter lists.[16] The secretary of state must prepare a public summary of the report as well as a confidential report for elected officials who are exempt from disclosure under the Texas Public Information Act.[17]

Cybersecurity Council and Select Legislative Committees

Cybersecurity Council. In the first quarter of 2018, the Texas Cybersecurity Council was established to assist with implementation of HB 8. The council is led by the state cybersecurity coordinator and also includes representatives from the offices of the governor, the lieutenant governor, and the speaker of the House of Representatives, private sector leaders, and representatives of institutions of higher education.[18] The Cybersecurity Council's requirement to establish a computer emergency readiness team, or CERT, is in progress, including a review of its costs and benefits. Additionally, the Cybersecurity Council will further implement HB 8 by establishing criteria for addressing cybersecurity threats; assessing the knowledge, skills, and capabilities of the existing state cybersecurity workforce; consolidating and synthesizing best practices; and providing recommendations to

the Legislature on legislation necessary to implement cybersecurity appropriate practices.[19]

Senate/House Committees on Cybersecurity. Finally, HB 8 calls for the creation of a Select Committee on Cybersecurity in both the House and Senate. Those committees must, either jointly or separately, study the information security plans of each state agency and the risks and vulnerabilities of state agency cybersecurity.

House Bill 9—the Texas Cybercrime Act

The Texas Cybercrime Act is a response to the lack of clearly defined criminal offenses related to cyberattacks, hacking, and other nefarious activity related to networks, devices, and digital information. The bill creates classes of criminal offenses for denial of service attacks, ransomware, and intentional deceptive data alteration.

Electronic Access Interference. The Cybercrime Act creates the offense of electronic access interference, a third-degree felony. A person commits this offense by intentionally interrupting or suspending access to a computer system or network without the effective consent of the owner.[20] Importantly, the definition of this crime includes a defense to prosecution if the person who took an action described above did so with the intent to facilitate lawful access to a computer network or system for a legitimate law enforcement purpose.[21]

Electronic Data Tampering and Ransomware. HB 9 defines "ransomware" as a computer contaminant or lock that restricts access, to an entire computer system or a computer file, by an unauthorized person to extort money from an authorized user and creates the offense of electronic data tampering.[22] A person commits this offense if the person intentionally alters data as it transmits between two computers through deception and without a legitimate business purpose or intentionally introduces ransomware onto a computer network or system through deception and without a legitimate business purpose.[23] The seriousness of this offense is dependent on the aggregate amount of financial losses involved, starting with a Class A misdemeanor for $100 or less and scaling up to a first-degree felony for $300,000 or more.[24] The starting point is raised to a state jail felony for an amount of $2,500 or less if it is shown that the defendant knowingly restricted a victim's access to privileged information.[25]

This legislation is a positive step in the process of modernizing the Texas Penal Code and provides law enforcement agencies in Texas with more robust tools for fighting cybercrimes. One key element of each of these new criminal statutes is the exception for legitimate business or law enforcement purposes. This important exception ensures that "white hat" operations, internal network security testing conducted by a company on its own network or devices, or legal law enforcement activities do not unintentionally subject employees, contractors, or law enforcement personnel to criminal liability.

House Bill 2087—Student Data Privacy Act

This legislation provides strong privacy protections for student data within Texas public schools. Digital learning resources and internet-connected technology are transforming the classroom experience and the overall learning environment.

However, along with the many benefits that digital tools offer, there are also new risks that must be addressed, especially with respect to student data. HB 2087 struck a balance between addressing those risks while being careful not to stifle the benefits that these new digital tools offer. The legislation was based on a model student privacy law that had previously been enacted, with some variations, in at least 14 other states.

The Student Privacy Act prohibits the sale or rental of any student's data,[26] bans targeted advertising to students based upon their use of educational services,[27] and prohibits the use of a student's data to build a student profile for any purpose other than an educational purpose.[28] These important prohibitions protect students' privacy while still allowing the flow of data and information inherently necessary for the utilization of digital learning technology.

HB 2087 generally prohibits disclosure of student data but also specifies when a third-party operator of an online service or application may permissibly disclose student data, including: to ensure legal or regulatory compliance; to protect against liability; to protect the safety and security of a website or application or the users of the website or application; for legitimate educational or research purposes; to comply with a request by the Texas Education Agency or a school district for a school purpose; and, with express consent of a student, to share data solely to provide access to employment, scholarships, or other educational opportunities for the student.[29]

The Student Data Privacy Act also specifies for what purposes an operator may use a student's data, which is essentially limited to educational purposes and to improve educational products, but only if no data will be associated with an identifiable student.[30]

Educational technology operators are also required to implement and maintain reasonable security procedures and practices designed to protect student data from unauthorized access, deletion, use, modification, or disclosure.[31] Lastly, an operator must delete student data whenever a school or school district requests that the data be deleted, unless the student or student's parent consents to the operator's continued maintenance of the student's data.[32]

Interactive websites and mobile applications have already changed the way that students, teachers, parents, and administrators interact with each other and the learning environment. These important privacy protections will allow such innovative technology to continue to thrive.

Senate Bill 1196—the Nuisance Website Act

SB 1196 authorizes an individual, the Texas attorney general, or a Texas district, county, or city attorney to bring a suit to declare that a person operating a web address or network of two or more computers is maintaining a common nuisance in certain circumstances.[33]

Nuisance Website Act actions may be brought under the Texas Civil Practice and Remedies Code against a person operating a web address engaging in: organized criminal activity as a member of a combination; prostitution, promotion of prostitution, or aggravated promotion of prostitution; compelling prostitution; sexual assault; aggravated sexual assault; continuous sexual abuse of a young child or children; massage therapy or other massage services in violation of business of which is the offering of a service or the selling, renting, or exhibiting of items intended to provide sexual stimulation or sexual gratification to the customer; trafficking of persons; sexual conduct or performance by a child; or employment harmful to a child.[34]

This legislation represents a novel attempt to combat human trafficking through innovative means and by extending the already-existing framework of nuisance law into the digital arena. The bill was crafted with the goal of substantially slowing down the rapidly

increasing use of websites and digital platforms to facilitate the practice of human trafficking. Law enforcement agencies now have an expanded arsenal of civil tools to shut down portals to criminal activity. Attorneys experienced in nuisance actions should be aware of this application of nuisance law.

House Bill 3593—Cybersecurity Education Act

The Cybersecurity Education Act, which went into effect on May 15, 2017, requires the State Board of Education to allow public school districts to offer cybersecurity courses for credit for high school graduation and to create language credits for coding courses.[35] In addition, a school district may offer a course about cybersecurity issues for credit without state board approval if it partners with one or more institutions of higher education to develop and provide the course.[36]

The act expands the New Instructional Facilities Allotment to renovate existing facilities for cybersecurity labs,[37] moves technical application courses under career and technical education, or CTE,[38] gives teachers a CTE certification subsidy, and lists cybersecurity and coding under the Science, Technology, Engineering, and Mathematics, or STEM, endorsement options.[39]

HB 3593 is an important step toward ensuring that the public education system in Texas is producing students equipped to be part of a 21st-century workforce. Understanding the various elements of cybersecurity and how to code are crucial skills for many jobs that exist today and even more that will exist in the future. The technology sector has grown by leaps and bounds in Texas in recent decades, and creating a pipeline of students who are familiar with cybersecurity and coding is a key element to continuing that growth.

Conclusion

The successful enactment of the Texas Cybersecurity Act, and a number of other laws in the 85th Legislature, shows that Texas is serious about addressing cybersecurity as a matter of public policy. The DIR has been given significant new responsibilities related to cybersecurity and will likely emerge as the go-to resource for such issues across Texas state government. The practical and immediate impact of HB 8 is that it elevates information network and data security as a top priority for state agencies and institutions of higher education in Texas. And the secretary of state is now expected to ensure that the state is following (and perhaps creating) adequate safeguards for election infrastructure. Given the vast amount of confidential and/or personally identifiable information held by state agencies, this legislation provided a critical response to the ever-evolving cyber threats present today.

The Texas Legislature is currently examining all of these issues closely via committees, the reports and studies required by HB 8, and the recommended priorities for the 86th Legislature that will be recommended by the Cybersecurity Council. Some trade associations are also weighing in to suggest a focus on requirements for local government and mandatory cybersecurity insurance for the public sector.

To effectively implement these new responsibilities, and those on the horizon, state agencies and institutions of higher education need to develop reliable internal and external resources. It is also important for state agencies and institutions of higher education to collaborate and coordinate among each other, and with the DIR, to sort through how best to comply with these myriad new responsibilities. Last, developing a network of subject matter experts will assist those impacted by HB 8 to comply with updated data breach notification procedures and Open Meetings Act exceptions. **TBJ**

The author would like to give a special thanks to Aaron C. Gregg, who is an associate in the Government, Law & Policy Practice Group at Greenberg Traurig, and to Tom Morgan, industry relations director at Qualia. Gregg has more than a decade of experience, before and after law school, in working at the Texas Capitol, including advising clients concerning privacy legislation. Morgan has been involved in providing governmental affairs strategy in a variety of industries for over a decade.

Notes

1. Joe Straus (@SpeakerStraus), Twitter (Apr. 25, 2017, 12:47 PM), https://twitter.com/SpeakerStraus/status/856927653454118912.
2. Tex. Gov't Code § 325.011(14).
3. *Id.* at § 2054.518.
4. *Information Security*, Texas Department of Information Resources, http://dir.texas.gov/View-About-DIR/Information-Security/Landing.aspx.
5. Tex. Gov't Code § 2054.0594.
6. *Id.* at 2054.076(b-1).
7. *Id.* at § 2054.515(c).
8. *Id.* at § 2054.575(a).
9. *See also* Tex. Admin. Code, ch. 202, which outlines specific information security standards those agencies must follow. *http://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202.*
10. Tex. Gov't Code § 2054.515(a-b).
11. *Id.* at § 2054.516.
12. *Id.* at § 2054.517.
13. *Id.* at § 551.089.
14. *Id.* at § 2054.1125(b).
15. *Id.*
16. Tex. Elec. Code § 276.011.
17. *Id.*
18. Tex. Gov't Code § 2054.512(a-c).
19. *Id.* at § 2054.512(d-e).
20. Tex. Penal Code § 33.022(a-b).
21. *Id.* at § 33.022(c).
22. *Id.* at § 33.023(a).
23. *Id.* at § 33.023(b).
24. *Id.* at § 33.023(d-1).
25. *Id.* at § 33.023(d-2).
26. Tex. Educ. Code § 32.152.
27. *Id.*
28. *Id.*
29. *Id.* at § 32.153.
30. *Id.* at § 32.154.
31. *Id.* at § 32.155.
32. *Id.* at § 32.156.
33. Tex. Civ. Prac. & Rem. Code § 125.0025.
34. *Id.* at § 125.0015(a).
35. Tex. Educ. Code §§ 28.002(f)(2), 28.025(b-12).
36. *Id.* at § 28.002(g-3).
37. *Id.* at § 42.158.
38. *Id.* at § 42.154(b).
39. *Id.* at §§ 28.025(c-10); 29.190(b).

ELIZABETH ROGERS
is a partner in the Privacy and Cybersecurity Practice Group of Michael Best & Friedrich. She was the first chief privacy officer in Texas state government and has firsthand experience working with the DIR in developing a state agency cybersecurity and privacy division.