Texas Association of School Boards
Legal Services
P.O. Box 400 • Austin, Texas 78767-0400 • 512.467.3610 • 800.580.5345 • legal.tasb.org • legal@tasb.org

Serving Texas Schools Since 1949

School Cybersecurity: Security Breach Notification and Response

Published online in TASB School Law eSource

This article answers basic questions about a school district's data breach notification and reporting requirements under Texas Education Code section 11.175 and Texas Business and Commerce Code chapter 521.

1. What type of data disclosure incident requires school districts to act?

When a district is made aware of unauthorized access to information it maintains, it may be required to act if the facts surrounding the circumstances meets the definition of a *breach of system security*.

Texas law provides two definitions for a *breach of system security* that districts need to consider.

Texas Education Code. Under the Texas Education Code, a *breach of system security* means an incident in which student information that is sensitive, protected, or confidential, as provided by state or federal law, is stolen or copied, transmitted, viewed, or used by a person unauthorized to engage in that action. Tex. Educ. Code § 11.175(a)(1).

Texas Business and Commerce Code. Under the Texas Business and Commerce Code, a *breach of system security* means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by the school district, including encrypted data if the unauthorized person has the key required to decrypt the data acquired. This does not include a good faith acquisition of sensitive personal information by an employee within the scope of employment for the purposes of the district unless the employee uses or discloses the sensitive personal information in an unauthorized manner. Tex. Bus. & Com. Code § 521.053(a).

Therefore, depending on what type of information is involved and how it was accessed, a district may be subject to legal obligations under both laws.

2. Under the Texas Education Code, what constitutes "student information that is sensitive, protected, or confidential, as provided by state or federal law"?

Texas Education Code section 11.175 does not provide definitions for what constitutes student information that is "sensitive, protected, or confidential, as provided by state or federal law". Tex. Educ. Code § 11.175(a)(1), (e). Without guidance from courts or the

attorney general, TASB Legal Services conservatively recommends a broad interpretation to include all information that is not considered subject to public disclosure under federal and state laws, and strongly encourages districts to consult with a school attorney when determining whether certain information is covered by the statute.

Examples of laws that are likely to apply include federal laws that govern student information, such as the Family Educational Rights and Privacy Act (FERPA) and the Individuals with Disabilities Education Act (IDEA). Examples of state laws that make various types of information confidential, including student information, include the Texas Public Information Act (PIA), the Texas Juvenile Justice Code, the Texas Education Code, and Texas Family Code chapter 261. These examples are not exhaustive.

The Texas Education Agency's (TEA) Cybersecurity Tips and Tools website offers a Sensitive Information Guideline containing examples of laws that districts may also review and consider when assessing whether a *breach of system security* has occurred under the Texas Education Code that requires the district to act.

3. Under the Texas Business and Commerce Code, what constitutes sensitive personal information?

The Texas Business and Commerce Code defines *sensitive personal information* as a person's first name or initial and last name in combination with the person's social security number, driver's license number or other government-issued identification number, or account number with a password or other access information that would allow access to the person's financial information. To qualify, the name and items must not be encrypted. The term also includes information that identifies a person and relates to his or her physical or mental health or personal condition, health care, or a health care payment. The term does not include publicly available information. Tex. Bus. & Com. Code § 521.002(a)(2), (b).

4. What must a school district do after discovering, or after receiving notification of, a *breach of a system security*?

Texas Education Code. If a cyberattack or other cybersecurity incident against school district cyberinfrastructure constitutes a breach of system security as defined by the Education Code, the school district's cybersecurity coordinator must provide notice to a parent, or person standing in parental relation of the student if the reported attack or incident involved an enrolled student's information. The cybersecurity coordinator must report the attack or incident to TEA or, if applicable, the entity that administers a system developed by the TEA and the Texas Department of Information Resource (DIR) to coordinate the anonymous sharing of information concerning cyber attacks or other cybersecurity incidents between participating schools and the state Tex. Educ. Code § 11.175(e), (f).

Texas Business and Commerce Code. If a district discovers or receives notification from another party about a breach of system security as defined by the Business and Commerce Code, the district must disclose any breach to any person whose sensitive personal information was, or is reasonably suspected to have been, acquired by an unauthorized person. The district must provide a similar notification to the owner or license holder of sensitive personal information if the district is maintaining the data. Tex. Bus. & Com. Code § 521.053(b); Tex. Loc. Gov't Code § 205.010(b).

In some cases, it may be unclear from a security incident whether the facts meet the definitions of a breach of system security or trigger required notification. Always consult your local school attorney for case-by-case analysis and guidance.

5. How should a school district report a breach of system security to TEA?

The district should report a breach of system security as defined by the Texas Education Code, to the following email address provided by TEA: cybersecurity@tea.texas.gov. For more information about breach notification to TEA, see TEA's Frequently Asked Questions TEA's Cybersecurity Tips and Tools website.

6. Why is a school district required to make a report as a *person* under the Texas Business and Commerce Code?

For the purpose of the Texas Business and Commerce Code, a person is defined as "an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, agency, or instrumentality, public corporation, any other legal or commercial entity, or a particular series of a for-profit entity." Tex. Bus. & Com. Code § 1.201(b)(27). A school district is a political subdivision of the state and a governmental entity. Consequently, a school district is subject to this law.

7. Does anyone else have a duty to provide notice of a breach?

Under Texas Business and Commerce Code, *any person* who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Tex. Bus. & Com. Code § 521.053(c).

Therefore, any school district employee, student, parent, volunteer, vendor, or other individual who is in possession of the school district's data containing sensitive personal information must notify the school district about any breach of system security immediately or be subject to the same penalties as a school district.

8. Are there any legal protections for a person who reports a district cybersecurity issue?

Yes. Any person who, in good faith, discloses to a state agency or other governmental entity, including a school district, information regarding a potential security issue with respect to the school district's information resources technologies is not liable for civil damages. However, this exemption would not apply if the person stole, retained, or sold any data obtained as a result of the security issue. Tex. Gov't Code § 2054.602.

9. How may a school district comply with breach notification requirements in the Business and Commerce Code?

A school district may provide the required notice in one of the following ways:

- Written notice at the last known address of the individual.
- Electronic notice, if the notice is provided in accordance with 15 U.S. C. § 7001 (concerning electronic records and signatures in commerce).
- If the district demonstrates that (1) the cost of providing notice would exceed $250,000, (2) the number of affected persons exceeds 500,000, or (3) the person does not have sufficient contact information, then the district may provide notice by:
  - Electronic mail if the district has electronic mail addresses for the affected persons;
  - Conspicuous posting of the notice on the district's website; or
  - Publication in or by broadcast on major statewide media.

Tex. Bus. & Com. Code § 521.053(e), (f).

10. How soon must a school district provide breach notification?

Texas Education Code. Reports by the school district's cybersecurity coordinator to the TEA, if required, must be made as soon as practicable after the discovery of each cyberattack or incident constituting *a breach of system security* as defined by the Texas Education Code. The Texas Education Code is silent as to how soon a district must provide parental notice, if such notice is determined to be required. Tex. Educ. Code § 11.175(e), (f).

Texas Business and Commerce Code. Under the Texas Business and Commerce Code, a district must give notice to all affected persons without unreasonable delay and in each case not later than the 60th day after the date on which the district determined that the breach occurred unless delay is authorized by law. Tex. Bus. & Com. Code § 521.053(b), (d). Additionally, the 60-day notice must be provided to the attorney general for each breach involving at least 250 Texas residents. Tex. Bus. & Com. Code § 521.053(i).

If the district must notify more than 10,000 people at one time, the district must also notify each national consumer reporting agency of the timing, distribution, and content of the notices without unreasonable delay. Tex. Bus. & Com. Code § 521.053(h).

11. For incidents involving at least 250 state residents, what does the notice to the attorney general require?

If an incident is subject to required notification to the attorney general under the Texas Business and Commerce Code, then the notice must include the following:

- a detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;
- the number of Texas residents affected by the breach at the time of notification;
- the number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification;
- the measures taken by the district regarding the breach;
- any measures the district intends to take regarding the breach after notification to the attorney general; and
- information regarding whether law enforcement is engaged in investigating the breach.

Tex. Bus. & Com. Code § 521.053(i).

12. When may a school district delay notification?

The district may only delay providing the required breach notification necessary to determine the scope of the breach and restore the reasonable integrity of the data system or at the request of a law enforcement agency because a law enforcement agency has determined notification will impede a criminal investigation. The notification then must be made as soon as the law enforcement agency determines that the notification will not compromise the investigation. Tex. Bus. & Com. Code § 521.053(b), (d).

13. May a school district adopt its own policy concerning the timing for notification?

Yes. A district complies with the timing requirements for notice under Section 521.053 if the district maintains its own information security policy and notification procedures for the treatment of sensitive personal information and the district notifies affected persons in accordance with its own policies and procedures. Tex. Bus. & Com. Code § 521.053(g).

14. What are the consequences for a school district that does not comply with the notification requirement?

Under the Texas Business and Commerce Code, the attorney general may bring an action to recover a civil penalty of at least $2,000 and up to $50,000 per violation from a school district that fails to comply with the notification requirement. The attorney general is entitled to reasonable expenses, including attorney's fees, court costs, and investigatory costs. Tex. Bus. & Com. Code § 521.151(a), (f).

In addition, the attorney general may bring an action to recover from a school district that fails to comply with the notification requirement a civil penalty of up to $100 for each individual to whom notification is due for each consecutive day that the district fails to take reasonable action to comply (for a maximum of $250,000 for all individuals for a single breach). Again, the attorney general is entitled to reasonable expenses, including attorney's fees, court costs, and investigatory costs. Tex. Bus. & Com. Code § 521.151(a-1), (f).

If it appears to the attorney general that a school district is engaging in, has engaged in, or is about to engage in conduct that violates the notification requirements, the attorney general may bring an action against the district to restrain or enjoin the violation. A court may grant any equitable relief the court considers appropriate to (1) prevent any additional harm to a victim of identity theft or a further violation or, (2) satisfy any judgment entered against the defendant. Tex. Bus. & Com. Code § 521.151(b), (e).

Meanwhile, Texas Education Code section 11.175 does not provide specific penalties. However, districts should bear in mind that the attorney general believes the Commissioner of Education is authorized to investigate violations of the Texas Education Code and take civil action as necessary. Tex. Att'y Gen. Op. No. KP-0254 (2019).

15. May a board deliberate about a cybersecurity breach in a closed meeting?

Yes, if the circumstances meet specific criteria for a closed meeting exception under the Texas Open Meetings Act, under the definitions of *cyber threat indicators* or *defensive measures* under the federal Cybersecurity Information Sharing Act (CISA), or under other law. Tex. Gov't Code ch. 551; 6 U.S.C. §§ 1501-1510. *See* Tex. Gov't Code §§ 551.089 (deliberation about certain security topics), 418.183(f) (deliberation about information covered by Tex. Gov't Code §§ 418.175-.182). A school district board considering discussing cybersecurity-related topics in closed meetings should consult its school attorney.

16. May school districts protect or withhold records and information pertaining to a cybersecurity breach incident from general public disclosure?

Yes, if the district complies with the procedures required under the PIA and other applicable laws governing release of district information to the general public. For example, certain information related to terroristic threats or homeland security activities is made confidential by Texas Government Code chapter 418 and certain cybersecurity information shared with a federal entity pursuant to the CISA is not subject to public disclosure under the PIA. E.g., Tex. Gov't Code ch. 418; 6 U.S.C. § 1504.

If a district has chosen to participate in the DIR's information sharing and analysis organization to exchange information regarding cybersecurity threats, best practices, and remediation strategies, then the district may not waive confidentiality of shared information and must assert legal exceptions to public disclosure under the PIA, specifically including Texas Government Code section 552.139, which protects confidential government information related to computer security or infrastructure. Tex. Gov't Code § 2054.0594(a), (c).

Additionally, different disclosure rules are likely to apply to requests not considered to be a public information request subject to PIA rules, such as requests from law enforcement, from contractual vendors assisting with an incident, or in the form of a valid subpoena. A school district that receives a request for information pertaining to a cybersecurity breach incident or investigation should immediately consult its school attorney.

17. Which TASB policies address data breach notification requirements?

TASB's model policy CQB addresses data breach notification requirements. TASB model policies BE and BEC summarizes open meeting requirements, and model policy GBA provides exceptions that may be claimed under the PIA. School districts facing an actual threat or active breach situations should contact law enforcement and work with their school attorneys and designated information security officer.

18. Is it also a crime for a person to breach a school district's computer security?

Yes. Computer and telecommunications-related crimes may be prosecuted under Texas Penal Code chapter 33. For instance, any person in Texas who knowingly accesses a computer, computer network, or computer system without the effective consent of the owner commits breach of computer security, which is a Class B misdemeanor or a state jail felony if (1) the defendant has been previously convicted two or more times of an offense under Texas Penal Code chapter 33, or (2) the computer, computer network, or computer system is owned by the government, including a school district, or a critical infrastructure facility. Tex. Penal Code §§ 1.07(a)(24), 33.02(a), (b). Furthermore, it is a crime for any person, with intent to defraud or harm another or alter, damage, or delete

property, to knowingly access a computer, computer network, or computer system without the effective consent of the owner or the government, including a school district, without authorization. Tex. Penal Code §§ 1.07(a)(24), 33.02(b-1). Depending on the circumstances, penalties can range from a Class C misdemeanor up to a first-degree felony. Tex. Penal Code § 33.02(b-2).

There is also a myriad of federal laws that may be used to prosecute cybercriminals, including but not limited to the Computer Fraud and Abuse Act, which generally makes it a crime to intentionally access a computer without authorization or in excess of authorized access to obtain information. 18 U.S.C. § 1030.

19. May we expend public funds to purchase cybersecurity insurance to protect the school district against liability resulting from system breach incidents?

Yes, a district may purchase insurance to protect itself and its board members from the cost and expense of defending litigation brought against them individually for acts or omissions committed by them in the good faith discharge of their official duties. A district may also, as an element of district employees' compensation, purchase necessary liability insurance in the name of such employees who are exposed to individual liability by virtue of their official duties. Tex. Att'y. Gen. Op. Nos. JH-0070 (1973), CM-0989 (1971). See TASB Policy CRB(LEGAL).

A school district may contact its insurance provider to determine whether coverage is available for data breach occurrences.

20. Are there other laws that may require districts to act upon discovering unauthorized disclosure of protected district information?

FERPA governs many aspects of *education records*, defined by the law as records maintained by a district that are directly related to a student or students. While FERPA does not technically require notification of breach incidents, it requires school districts to document each request for access to and each disclosure of personally identifiable information (PII) from the education records of each student, as well as the names of state and local educational authorities and federal officials and agencies (authorized by law) that may further disclose PII from student records without certain consent. 34 C.F.R. § 99.32(a)(1). The U.S. Department of Education has recommended that schools provide direct student notification when compromised data includes student social security numbers and other identifying information that could lead to identity theft. FERPA Final Rule, 73 Fed. Reg. 237 (Dec. 9, 2008); 34 C.F.R. pt. 99.

The Texas Medical Records Privacy Act (MRPA) requires a covered entity to provide notification to individuals for whom the covered entity creates or receives protected health information (PHI), such as employee medical records, if the individuals' PHI is

subject to electronic disclosure. Tex. Health & Safety Code §§ 181.001-182.155. It is unclear, however, whether the definition of *covered entity* under the MRPA includes a local governmental entity such as a school district. One county governmental entity requested an opinion from the attorney general, but no opinion has been issued to date. *See* Attorney General of Texas, Pending Opinion Request RQ-1105-GA (Jan. 25, 2013) (requesting the attorney general's opinion as to whether a county is a "covered entity" under Texas Health and Safety Code section 181.001(b)(2) and is subject to the Health Insurance Portability and Accountability Act). A school district with questions about notice requirements related to breach of PHI should consult its school attorney to determine applicability of the MRPA to its district.

The General Data Protection Regulation (GDPR), an international privacy rule that governs personal information of European Union (EU) residents, has garnered much attention for its intent to reach data privacy violators around the world. Although the European regulation has minimal, if any, direct practical impact on U.S. public schools, especially if they do not process personal information of EU residents in the EU, it is worth noting that the GDPR contains a 72-hour breach notification requirement. A school district concerned about its data processing activities involving students or employees residing in an EU country, such as potential foreign-exchange student applicants or employment candidates, should consult its school attorney to determine applicability of the GDPR to its district in the case of a data breach.

This document is continually updated at tasb.org/Services/Legal-Services/TASB-School-Law-eSource/Business/documents/school-cybersecurity-security-breach-notification-and-response.pdf. For more information on school law topics, visit TASB School Law eSource at schoollawesource.tasb.org.

Updated September 2021