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: Getting Started

*Published online in TASB School Law eSource*

School cyberattacks disrupt learning, divert student resources, and subject victims and districts alike to costly recovery efforts. This article examines cybersecurity risk management, common cyberattack methods, primary laws governing school cybersecurity, and how board members may begin to address the online security needs of their districts.

For cybersecurity requirements specific to Texas school districts, see TASB Legal Services' *School Cybersecurity: Texas Requirements* and *School Cybersecurity: Security Breach Notification and Response*.

## 1. What is cybersecurity?

Texas law specifically defines *cybersecurity* to mean the measures taken to protect a computer, computer network, or computer system against unauthorized use or access.[1]

## 2. What is the difference between "privacy" and "security"?

Although privacy and security are interconnected ideas in practical application, they are often discussed by experts as two distinct concepts addressed by different laws.

Data "security" broadly involves ensuring information is kept safe.[2] For the purpose of this article, the term "security" refers to the technical and operational aspects of protecting data from breach or illegal intrusions by criminals and other unauthorized users. On the other hand, data "privacy," which will not be discussed in this article, generally refers to the idea of managing—but allowing—disclosures of data as authorized by law or consent.

## 3. What is cybersecurity risk management?

A 2017 presidential executive order described *cybersecurity risk management* as "the full range of activities undertaken to protect internet technology (IT) and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents."[3]

---

1 Tex. Educ. Code § 11.175(a)(3).

2 *Glossary*, U.S. Dep't of Education, Privacy Technical Assistance Center.

3 Exec. Order No. 13800, 82 Fed. Reg. 22,391 (May 11, 2017).

© 2021. Texas Association of School Boards, Inc. All rights reserved.

A comprehensive cybersecurity risk management program in a public school district aims to prevent harm to various data systems—from employment to enrollment, food and nutrition to transportation logistics, and many other critical school services. A school cybersecurity risk management program should aim for a continuous cycle of assessing for risk vulnerabilities, detecting potential threats, providing education and training, and responding quickly to attacks and recovery efforts. Likewise, board governance may involve routine reviews of such cycles of:

- assessment (to identify cybersecurity risks);
- prevention (to reduce risks with technical measures and user education); and
- preparation for mitigation and recovery (in case of an actual incident).

**4. What challenges do districts generally face in managing cybersecurity risk and how may districts overcome those challenges?**

Schools may find themselves vulnerable to cyberattacks and other cybersecurity challenges because schools are often attractive targets to cybercriminals. Schools often collect a broad range of personal data, are susceptible to multiple points of vulnerability, employ an overtasked workforce, educate a most trusting age group, and may have underfunded security systems. Advances in technology pose extra challenges for school districts due to the sheer volume of data that is created, the different formats in which data exists, and the multiplicity of originating data sources. Many districts lack ready resources to ensure consistent oversight of a cybersecurity management program, which adds to existing challenges. However, as technology continues to modify traditional solutions to data security, schools must adapt to new approaches to secure new forms of data in intangible, digital environments.

**5. What is a cyberattack?**

A *cyberattack* is any attempt to damage, disrupt, or gain unauthorized access to a computer, computer network, or computer system.[4]

**6. What are some common cyberattacks that school districts may face?**

The U.S. Department of Education, Readiness and Emergency Management for Schools (REMS) Technical Assistance Center (TAC) cites the following types of online threats as most common for school districts:[5]

---

[4] Tex. Educ. Code § 11.175(a)(2).

[5] *See* Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center, *Cybersecurity for Schools Fact Sheet*. *See also* Tiina Rodrigue, Senior Advisor for Cybersecurity, U.S. Department of Education Federal Student Aid office, Cyber Advisory Letter (Oct. 16, 2017) (explaining that, in extreme instances, cybercriminals have resorted to threats of violence and extortion against districts and students).

© 2021. Texas Association of School Boards, Inc. All rights reserved.

**Data breaches.** A data breach involves disclosure of sensitive, personal, confidential, or other protected data in an unauthorized manner. Examples include when school data is:

1. Inadvertently released without authorization;
2. Intentionally accessed by someone without authorization;
3. Legally released to third parties who then fail to protect the information;
4. Physically unprotected when school equipment is stolen or lost; or
5. Intentionally accessed by someone with authorization but used without a legitimate educational interest or for unauthorized purposes.

These breaches may occur if private data is transferred onto personal devices or transmitted using unencrypted servers. Malicious actors can easily exploit users who lack security awareness training or environments which are infrequently updated or feature poor security controls. Lax agreements with third-party vendors can also leave confidential information exposed to unauthorized users or lead to instances of physical data misappropriation.

**Denial of service attacks.** A Denial of Service (DoS) attack, sometimes also referred to as a Distributed Denial of Service (DDoS) attack, occurs when a school's website is deliberately overloaded with requests so that the website shuts down. Users are then unable to access the website. This may also affect the entire district network and halt network-based operations.

**Phishing scams.** *Phishing* is a form of social engineering, which involves using electronic communication to solicit information from a victim or drive action by the victim. Phishing scammers may pose as a trustworthy source or organization to trick a recipient to open a file or link, reveal sensitive information, provide access credentials or physical access, schedule a meeting, or process requests on behalf of the scammer.

*Spear phishing* or *whaling* is a specific form of phishing that occurs when a scammer impersonates an executive or supervisor to target an employee for illegitimate gains. For example, an email may appear to come from the superintendent requesting copies of all employee social security numbers or asking the recipient to log in to a shared file using current passwords.

*Phone/Voice phishing* occurs when a scammer tricks the victim into believing that a call is coming from a legitimate person or organization requesting sensitive information, such as spoofing a phone number to trick caller identification devices. For example, a phishing call may appear to be from a school district asking taxpayers to provide their bank account numbers for a tax refund.

© 2021. Texas Association of School Boards, Inc. All rights reserved.

*SMS phishing* occurs, similarly, by means of text messages. For example, a phishing text may ask a parent to click on the link to access their student's grades or to deposit money for lunch accounts.

**Malware.** Malware is a general term that covers various kinds of malicious software programs, including ransomware, used by criminals to gain access to a victim's computer or computer systems. Cybercriminals use malware to damage or disables computer system functionalities in order to demand something of value from the victim. Examples of malware include:

*Ransomware*, also known as *lockerware*, uses software to encrypt the victim users' files or locks entry to computer systems until a payment demand is fulfilled by the user.

*Viruses, worms, Trojans, spyware,* or *adware* are various kinds of malware that force an unwanted action on the computer system or user to cause harm, often with the hope of some benefit or value to the originating bad actor.

Malware can be delivered not only in email scams or seemingly legitimate websites containing malicious computer codes, but also by means of data carriers like thumb/flash drives, CD-ROMs, or other portable storage devices, and outdated protection software.

**Unpatched or Outdated Software.** The sheer number of ongoing software patches and hardware updates can often paralyze an organization, keeping them from implementing the most critical of repairs and updates. When a patch or update is not implemented, malicious cyberattackers can remotely exploit the existing vulnerabilities resulting from poor patching cadence to gain access to school networks, applications and systems. To minimize risks associated with poor patching cadence, school districts should make every effort to regularly update devices, servers, and other assets as soon as possible after a patch is released. Schools with limited resources may consider automating the patching process to improve their security posture.

**Mismanagement of Mobile Devices and Portable Technology.** Removable devices that can be connected to computers, such as USB drives, CD-ROMs, DVDs, and external hard drives, as well as electronic devices such as laptops, tablets, and mobile phones, also pose challenges to school cybersecurity. Not only are such storage devices easily stolen, but malware-infected devices can also be unwittingly connected to district computers and networks that, once opened, further infect other devices or spread quickly across the entire network. For example, a teacher who plugs an infected USB drive into a school computer or virtually transfers an infected file from an unapproved third-party cloud storage provider (such as Dropbox) can infect the entire school network.

© 2021. Texas Association of School Boards, Inc. All rights reserved.

It is no surprise that cyberattacks are considered "Adversarial, Incidental, and Human-caused Threats," a category shared with fire, active shooters, criminal threats or actions, gang violence, bomb threats, domestic violence and abuse, and suicide, according to the REMS TA Center.[6]

**7. What can schools do to reduce their vulnerability to cyberattacks?**

The U.S. Department of Education's Privacy Technical Assistance Center (PTAC) advises schools and districts to take the following minimum steps to establish cybersecurity preparedness:[7]

1. conduct security audits to identify weaknesses and update/patch vulnerable systems;
2. create and routinely review audit logs for suspicious activity;
3. train staff and students on data security best practices and how to recognize social engineering tactics by scammers; and
4. limit access to sensitive data.

The FBI recommends that organizations focus on two main areas to reduce risk of malware attacks:[8]

1. prevention efforts (such as awareness training and robust technical prevention controls); and
2. creating a solid operations continuity plan in case of an attack.

TASB Risk Management Fund recommends designating an information security officer (ISO) who, when possible, has information security duties as their primary role and responsibility and has the explicit authority to administer data privacy and cybersecurity requirements on behalf of the district's board, superintendent, or other relevant executive level management. The ISO should be tasked with developing and maintaining a cybersecurity plan that includes appropriate information security policies, procedures, and technical controls. Additionally, the officer should provide guidance and assistance to board members, information-owners, information custodians, and end users concerning their independent responsibilities in combating cyber risk.

The Texas Department of Information Resource has developed a Security Plan Template, which can be leveraged to build the district's cybersecurity plan. This resource establishes 40 distinct security objectives (controls) and provides the opportunity for

---

6 REMS TA Center, *Guide for Developing High Quality School Emergency Operations Plans* (June 2013).
7 U.S. Dep't of Educ., PTAC, Cyber Advisory – New Type of Cyber Extortion/Threat Attack (Oct. 2016).
8 FBI website, Cyber Crime.

© 2021. Texas Association of School Boards, Inc. All rights reserved.

districts to use a common language to address and manage cybersecurity risk in a cost-effective way, without burdening districts with additional regulation. Using the plan template as a guiding tool, a school district may conduct a thorough inventory of all information systems; review related ownership and responsibilities; and coordinate the review of data security requirements, specifications, and third-party risk assessments of any new or existing computer applications or services that receive, maintain or share confidential data. A school board may request periodic reports on the status and effectiveness of the security control implementation.

**8. Does an individual incur liability for reporting cybersecurity concerns to the school district?**

No. A person who in good faith discloses to a governmental entity information regarding a potential security issue with respect to the entity's information resources technologies is not liable for any civil damages resulting from disclosing the information unless the person stole, retained, or sold any data obtained as a result of the security issue.[9]

**9. What other laws related to cybersecurity apply to schools?**

**Federal Law.** Most laws regulating cybersecurity apply at the federal level or in private sectors to entities directly involved in securing the nation's critical infrastructure. In 2015, however, Congress passed the Cybersecurity Act to enhance the ability of governmental agencies to fight cybercrimes and protect national security. In Title I of the Cybersecurity Act of 2015, known as the Cybersecurity Information Sharing Act (CISA), schools and other non-federal entities, including private companies, were authorized to cross-share information related to cyber threat indicators and defense measures between and among all levels of federal government under certain conditions.[10]

Under the CISA, school districts may share or provide cyber-threat information with federal agencies without facing legal liability or being subject to open government laws, loss of proprietary protections, or concerns about waiving privilege or engaging in *ex parte* communication. If a school district chooses to share such cybersecurity threat information under the CISA, it must remove any personal information not directly related to a cybersecurity threat. See TASB Policy CQB(LEGAL). For more information, see Dept. of Homeland Security, The Dept. of Justice, *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015* (June 15, 2016).

**State Law.** Many Texas laws directly affect the management of school cybersecurity, discipline of students engaged in cyber-related misbehaviors, and reporting of cybercrimes to local law enforcement.

---

[9] Tex. Gov't Code § 2054.602.

[10] 6 U.S.C. §§ 1501-1510.

© 2021. Texas Association of School Boards, Inc. All rights reserved.

*Required Notification of Data Breach.* As noted above, a school district must report any cyberattack or other cybersecurity incident against the district cyberinfrastructure that constitutes a breach of system security. Additionally, the Texas Business and Commerce Code requires school districts to provide notification of breaches in their system security if circumstances meet requisite conditions.[11] Read more about these requirements at TASB Legal Services': *School Cybersecurity: Security Breach Notification and Response*.

*Voluntary Participation in Cybersecurity Information Sharing*. School districts may choose to participate in an information sharing and analysis organization established by DIR to provide a forum for information regarding cybersecurity threats, best practices, and remediation strategies. This forum can be for state agencies, local governments (including school districts), public and private institutions of higher education, and the private sector. The forum may establish a list of available cybersecurity experts and share resources to assist in responding to the cybersecurity event and recovery from the event.[12]

Participants in this group may not waive confidentiality to shared information in response to any non-participant requests and must assert legal exceptions to public disclosure under the Texas Public Information Act, specifically including Section 552.139 of the Texas Government Code which protects confidential government information related to computer security or infrastructure.[13]

School districts may also participate in an anonymous information sharing system between participating schools and the state that is developed by TEA, in coordination with DIR, concerning cyberattacks or other cybersecurity incidents.[14]

*Disciplining Students for Cybersecurity Misbehaviors*. A district may expel a student for engaging in conduct that contains the elements of the offense of breach of computer security under Texas Penal Code section 33.02 if:

1. the conduct involves accessing a computer, computer network, or computer system owned by or operated on behalf of a school district; and
2. the student knowingly:
    a. alters, damages, or deletes school district property or information; or
    b. commits a breach of any other computer, computer network, or computer system.[15]

---

11 Tex. Educ. Code § 11.175. Tex. Bus. & Com. Code §§ 521.001-.152.
12 Tex. Gov't Code § 2054.0594(a), (d).
13 Tex. Gov't Code § 2054.0594(c).
14 Tex. Educ. Code § 11.175.
15 Tex. Educ. Code § 37.007(b)(5). See TASB Policy FOD(LEGAL).

© 2021. Texas Association of School Boards, Inc. All rights reserved.

*Punishing Cybercriminals*. In addition to federal laws penalizing prohibited internet- or computer-related activities, which will not be reviewed in this article, state law such as Texas Penal Code chapters 33 (for computer crimes) and 33A (for telecommunications crimes) specifically penalize cybercriminals. Under chapter 33, districts may wish to report to law enforcement conduct constituting computer crimes, such as breach of computer security, online solicitation of a minor, electronic access interference, electronic data tampering, unlawful decryption, tampering with direct recording electronic voting machine, and online impersonation.[16]

Under Chapter 33A, districts may also report conduct constituting telecommunications crimes, such as unauthorized use of a telecommunications device, manufacture, possession, or delivery of an unlawful telecommunications device, theft of telecommunications device, and publication of telecommunications access device.[17]

Under both Chapters 33 and 33A, prosecutors may obtain assistance from the attorney general.

**10. What is the role of a school board in reducing cybersecurity risks?**

Cybersecurity governance begins with asking and answering fundamental questions:

a. **What do we have that needs protecting?** Know what it is you are protecting.
b. **Where do we have it?** Know where your vulnerabilities are located.
c. **How do we provide protection?** Know how to remedy vulnerabilities, whether it is tangible or knowledge based.
d. **What should we do if there is an incident?** Know the required and recommended response to incidents.

School boards can positively impact a district's cybersecurity risk management efforts by:

- Adopting local policies that promote responsible use of school technology resources and networks and that set sensible limits on the use of personal telecommunication/electronic devices. See TASB Policies BBI, CQ, DH, and FNCE.
- Completing cybersecurity training and selecting appropriate cybersecurity training for all employees. See TASB Policy CQB.
- Encouraging the reporting of suspicious activities that may indicate data breach or other cybersecurity incidents. See TASB Policy CQB.

[16] Tex. Penal Code §§ 33.01-.07.
[17] Tex. Penal Code §§ 33A.01-.05.

© 2021. Texas Association of School Boards, Inc. All rights reserved.

- Directing the development of a cybersecurity crisis plan or incident response protocol. See TASB Policy CKC.
- Ensuring the district securely stores sensitive data and properly controls access to networks and systems. See TASB Policy CQB.
- Encouraging cybersecurity awareness training beyond what's required by law for everyone, including vendors, board members, students, employees, and volunteers. See TASB Policy GKG.
- Promoting and supporting an active records management program, which allows for destruction of data in compliance with records retention schedules to reduce the amount of personal or sensitive information available to a successful cybercriminal seeking to misuse data, and assessing the program's efficacy. See TASB Policy CPC.
- Generally educating the community on the district's efforts to remain cyber-secure in a digital-information age and encouraging timely reporting to the district of any suspicious cyber activities.

**11. May school boards deliberate cybersecurity concerns in a closed meeting?**

Yes, if the circumstances meet specific criteria for a closed meeting exception under the Texas Open Meetings Act, Texas Government Code chapter 551, CISA's definitions of *cyber threat indicators* or *defensive measures*, or any other law.[18]

A school board considering discussing cybersecurity-related topics in closed meetings should consult its school attorney.

**Conclusion**

Ultimately, cybersecurity is not only a concern for public education, but also a national and international challenge. As leaders of learning institutions, school boards are well-positioned to devise defenses from the heart of the solution: our schools, our staff, and our students.

**Additional Resources**

There are many online resources available that provide additional guidance to school districts for developing cybersecurity plans. Below are some good starting points:

*Federal/National*

- U.S. Department of Education (DOE)'s Privacy Technical Assistance Center (PTAC) offers data security and breach response checklists, best practices, training exercises, and more.

[18] Tex. Gov't Code ch. 551; 6 U.S.C. §§ 1501-1510. *See also*, e.g., Tex. Gov't Code §§ 551.089 (deliberation about certain security topics) and 418.183(f) (deliberation about information covered by Texas Government Code sections 418.175-.182).

© 2021. Texas Association of School Boards, Inc. All rights reserved.

- National School Boards Association (NSBA)'s Cyber Secure Schools offers resources for cybersecurity planning, policy development, suggestions for cyber-related career pathways, and more.
- U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) offers a variety of resources in support of its mission to protect the nation's critical infrastructure, including schools, from physical and cyber threats.
- U.S. Department of Homeland Security's Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center offers suggestions for overall cybersecurity preparedness and emergency response, and more.
- Federal Bureau of Investigation's Cyber Division investigates cybercrimes and provides helpful tips on counteracting criminal efforts.
- Internet Crime Complaint Center (IC3) provides a reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated fraud schemes.
- National Center for Education Statistics (NCES) collects and analyzes date related to U.S. education and offers various publication on education data privacy and practical guidelines for education information security, and more.
- National Institute of Standards and Technology (NIST)'s Cybersecurity Framework provides a model cybersecurity risk management tool that may be used to identify, assess, and manage cybersecurity risk.

*Texas*

- Texas Education Agency (TEA)'s Cybersecurity Tips and Tools offers sample information security policies, data breach practice, suggestions for training resources, and more.
- Texas Department of Information Resources (DIR)'s Cyber Texas website provides information about cybersecurity and related issues.
- Texas Department of Information Resources (DIR)'s Cybersecurity Council is a private industry-government council that implements recommendations and initiatives related to cybersecurity.
- Texas Association of School Boards (TASB) Legal Services' eSource library offers a variety of articles and resources related to schools and technology, and more.
- TASB Risk Management Fund offers free consultation to Fund Property and Liability members, as part of existing coverage, regarding data privacy and cybersecurity challenges, as well as resources and information pertaining to cybersecurity awareness and training.

© 2021. Texas Association of School Boards, Inc. All rights reserved.

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

*This document is provided for educational purposes only and contains information to facilitate a general understanding of the law. It is not an exhaustive treatment of the law on this subject nor is it intended to substitute for the advice of an attorney. Consult with your own attorneys to apply these legal principles to specific fact situations.*

*Updated September 2021*

© 2021. Texas Association of School Boards, Inc. All rights reserved.
TASB Legal Services