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

From data thieves stealing identities or locking systems to demand ransom, to online predators preying on students or trafficking minors, cyberattacks against schools not only disrupt learning and divert resources from students but also subject victims and districts to costly recovery efforts. This article briefly examines what cybersecurity risk management means for Texas schools, common cyberattack methods, primary laws governing school cybersecurity, and how board members may begin to address the online security needs of their districts.

Q: What is cybersecurity?

A: *Cybersecurity* can be thought of as a broad range of offensive and defensive practices, tools, and ideas relating to an organization's informational, operational, and technical security. The "cyber" term simply reflects today's digital environment.

The U.S. Department of Homeland Security defines *cybersecurity* more specifically as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." National Initiative for Cybersecurity Careers and Studies, U.S. Department of Homeland Security, *Glossary* (Sept. 11, 2018).

Q: What is the difference between cyber-privacy and cyber-security?

A: For the purpose of this article, data "security" or "cybersecurity," when data is located on the Internet or in a virtual environment, refers to the technical and operational aspects of protecting such data from breach or illegal intrusions by criminals and other unauthorized users. Informally, security may be thought of as protecting data from external attackers or malicious insiders by ensuring data confidentiality, integrity, and availability ("data CIA"), which is accomplished through robust policies, procedures, and supporting technical controls. Advances in technology can pose extra challenges to the data CIA paradigm, however, due to the sheer volume of data that is created and that needs to be protected, the many different formats in which data exists, and the multiplicity of originating data sources, thanks to the Internet of Things (IoT). Many district also lack resources to ensure consistent oversight, which only adds to the existing challenge of securing the district's data. Nonetheless, as technology continues to modify traditional solutions to data security, such as manual sealing of an envelope or locking a metal file cabinet, schools must also adapt to new ways of thinking about how to secure new forms of data in intangible, digital environments.

Data "privacy," which is not discussed in this article, only addresses the confidentiality component of the "data CIA" triad framework, and generally refers to the idea of protecting data confidentiality by managing proper disclosures to authorized parties. Although privacy and security are interconnected ideas in practical application, they are often discussed as two distinct concepts and addressed by different laws.

Q: What is cybersecurity risk management?

A: In a 2017 executive order, the president 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." Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (May 11, 2017).

In simpler terms, a comprehensive cybersecurity risk management program in a public school environment protects its data systems by engaging in a continuous cycle of assessing for risk vulnerabilities, detecting potential threats, providing education and training, and timely responding to attacks and recovery efforts.

Q: What are some examples of common cyberattacks that school districts may face?

A: The U.S. Department of Education, Readiness and Emergency Management for Schools (REMS) Technical Assistance Center (TAC), crediting the FBI and the Department of Defense's Defense Technical Information Center, cites the following types of online threats as most common or likely for school districts:

- **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 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 physical instances of 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 occur to the entire district network and halt network-based operations.
- **Phishing scams.** *Phishing* is a form of social engineering, which uses 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.
  - *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. Malware usually damages or disables computer system functionalities in order to benefit from the victim. Examples of malware include:
  - *Ransomware*, also known as *lockerware*, which 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, or outdated protection software.

- **Unpatched or Outdated Software.** The sheer number of ongoing software patches and hardware updates can often paralyze an institution, keeping them from implementing the most critical of repairs and updates. When a patch or update is not implemented, malicious cyber attackers can remotely exploit the existing vulnerabilities, which exist as a result of 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 flash 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 be unwittingly connected to district computers and networks that, once opened, further infect other device or spread quickly across the entire network. For example, a teacher who plugs an infected thumb 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.

  Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center, *Cybersecurity for Schools Fact Sheet*.

  See 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).

  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. REMS TA Center, *Guide for Developing High Quality School Emergency Operations Plans* (June 2013).

Q: What can schools do to reduce their vulnerability to cyberattacks?

A: Cybercriminals may find schools to be attractive targets for many reasons. Schools often collect a large volume and broad range of personal data, have many points of vulnerability, employ an overtasked workforce, educate a most trusting and vulnerable age group, and are more likely to operate underfunded security systems.

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

(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.

PTAC, *Cyber Advisory – New Type of Cyber Extortion/Threat Attack* (Oct. 2016).

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

(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.

FBI, *Cyber Crime*.

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, which 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 Resources (DIR) 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 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 as a guiding tool, the ISO may conduct a thorough inventory of all information systems, 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. The ISO should report to the board, at least annually, on the status and effectiveness of the security control implementation.

Q: What cybersecurity laws apply to schools?

A: **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. 6 U.S.C. §§ 1501-1510. Under the CISA, school districts may share or provide cyber threat information 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 CQ(LEGAL).

For example, if a district wanted to share information from a spear phishing email incident, the personal information about the email sender, attached malware files, and other information about that email may be considered a cyber threat indicator. In the same example, the personal information of email recipients (such as name and personal email address) would generally be considered personal information not directly related to a cybersecurity threat. For more information on the CISA, see Department of Homeland Security, The Department 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.

Required Notification of Data Breach

Texas Business and Commerce Code chapter 521, Unauthorized Use of Identifying Information, requires school districts to provide notification of breaches in their system security (commonly referred to as data breaches). Tex. Bus. & Com. Code §§ 521.001-521.152. Read more about this requirement at TASB Legal Services' *School Cybersecurity: Security Breach Notification and Response*.

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, schools 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. Tex. Pen. Code §§ 33.01-33.07. Under chapter 33A, schools 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. Tex. Pen. Code §§ 33A.01-33A.05. Under both chapters 33 and 33A, prosecutors may obtain assistance from the attorney general.

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:

(A) the conduct involves accessing a computer, computer network, or computer system owned by or operated on behalf of a school district; and

(B) the student knowingly:

  (i) alters, damages, or deletes school district property or information; or

  (ii) commits a breach of any other computer, computer network, or computer system.

Tex. Educ. Code § 37.007(b)(5). See TASB Policy FOD(LEGAL).

Q: What does cybersecurity risk management or governance mean for school boards?

A: Governing the cybersecurity of schools often involves management of two major components of school operations. One is to manage information found in physical records. The other is to manage the gambit of information held by technology systems, software, devices and digital applications. Doing both involves properly configuring, securing, and proactively managing an array of hardware and software components. School districts must adequately engage in an ongoing cycle of assessment to identify cybersecurity risks, prevention to reduce risks with technical measures and user education, and planning for potential mitigation and recovery in case of an actual incident.

In the simplest terms, cybersecurity governance begins with asking and answering fundamental questions:

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

Effective cybersecurity risk management will require districts to engage leaders from all departments, identify areas of vulnerability, integrate prevention measures into every aspect of district operations, and educate individuals at all levels. For instance, boards and districts may want to consider reducing cybersecurity risk management by planning for a more rigorous "front-end" procurement process where preventative measures like third-party contract terms and software support are built into the beginning of a purchasing process, prior to committing funds and building dependency on a product or service, rather than relying on resolving disputes on the "back end" of a binding agreement when harm has occurred or payment already made, when legal disputes become more costly. Training for employees and students about how to recognize fraudulent activities online may reduce the probability of cyberattacks. And, ensuring regular review of how the district uses its technology resources can ensure adequate planning and support for protecting those resources.

As part of their cybersecurity risk reduction efforts, boards and districts should also assess the efficacy of their records management program, which allows for destruction of data in compliance with records retention schedules and can reduce the amount of personal or sensitive information available to a successful cybercriminal seeking to misuse data.

Q: What is the role of a school board in reducing cybersecurity risks?

A: School boards are critical to every aspect of strengthening the cybersecurity of their districts and 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.
- Developing 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 CQ.

- Supporting regular cybersecurity awareness training for board members, students, employees, and volunteers. See TASB Policy GKG.
- Promoting and supporting an active records management program. 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.
- Designating a person to be responsible for a district cybersecurity program that encompasses all of the above considerations.

Q: May school boards deliberate cybersecurity concerns in a closed meeting?

A: Yes, if the circumstances meet specific criteria for a closed meeting exception under the Texas Open Meetings Act, Tex. Gov't Code chapter 551, or under CISA's definitions of *cyber threat indicators* or *defensive measures*. A school district considering discussing cybersecurity-related topics in closed meetings should consult its school attorney.

Q: How may school boards provide their students a career pathway in cybersecurity?

A: As technology becomes more sophisticated and market demand for cyber-related skills increases, all industries including the government are turning to schools to supply a workforce with cybersecurity skills and knowledge. Researchers project that the nation will face a shortage of 1.5 million cybersecurity professionals by year 2020. Institute for Critical Infrastructure Technology, *Sowing the Seeds of U.S. Cyber Talent* (Apr. 2017).

Under Texas Education Code chapter 28, school boards may authorize local course credit for cybersecurity courses that counts toward graduation as approved by the State Board of Education (SBOE). Approval from the SBOE is not required if the district partners with an institution of higher education that offers an undergraduate degree program in cybersecurity to develop and provide courses. Tex. Educ. Code § 28.002(f)(2), (g-3). Students may also substitute credits in computer programming languages and coding for credits in a language other than English required for graduation, and choose a cybersecurity pathway under the STEM (science, technology, engineering, and mathematics) endorsement as approved by the SBOE. Tex. Educ. Code § 28.025 (b-12), (c-1).

Additionally, districts may apply for a subsidy from the Texas Education Agency (TEA), subject to approval by the commissioner of education, to recover the cost of a certification exam it paid for any teacher who passes a certification examination related to cybersecurity. To obtain reimbursement for a subsidy paid under this section, a district must pay for the examination fee and then submit a written application for reimbursement on a form prescribed by the commissioner. Tex. Educ. Code § 29.190(b), (c).

Finally, schools entitled to a new instructional facility allotment under Texas Education Code section 42.158 may use the funds to renovate an existing instructional facility to serve as a dedicated cybersecurity computer laboratory. Tex. Educ. Code § 42.158(a-1).

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 conquer these battles from the heart of the solution: our schools.

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.
- **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 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.

This document is continually updated, and references to online resources are hyperlinked, at https://tasb.org/Services/Legal-Services/TASB-School-Law-eSource/Business/documents/school-cybersecurity-getting-started.pdf. For more information on this and other school law topics, visit TASB School Law eSource at schoollawesource.tasb.org.