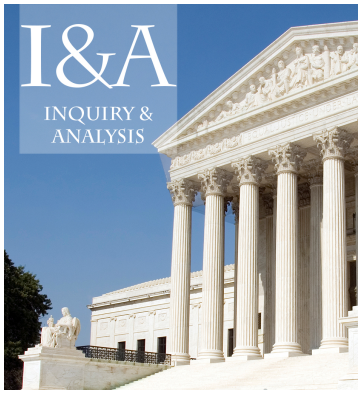
National School Boards Association

cosa

Council of School Attorneys



August 2016 Inquiry & Analysis

A Membership Service of the NSBA Council of School Attorneys

Tammy Carter, *Editor and Senior Staff Attorney*

NSBA Council of School Attorneys 2016-17 Officers
Andrew M. Sanchez, *Chair*
Pilar Sokol, *Chair-elect*
Diane Marshall-Freeman, *Vice-chair*
Phillip L. Hartley, *Secretary*

NSBA Officers and Staff
Miranda A. Beard, *NSBA President*
Kevin E. Ciak, *President-elect*
Frank C. Pugh, *Secretary-Treasurer*
John D. Tuttle, *Immediate Past President*
Thomas J. Gentzel, *NSBA Executive Director*
Marie S. Bilik, *NSBA Deputy Executive Director*
Francisco M. Negrón, Jr., *NSBA Associate Executive Director and General Counsel*
Sonja H. Trainor, *Director, Council of School Attorneys*
Naomi E. Gittins, *Deputy General Counsel*
Leza Conliffe, *Senior Staff Attorney*
Tammy T. Carter, *Senior Staff Attorney*
Lyndsay Andrews, *Manager, Council of School Attorneys*
Thomas Burns, *Paralegal*
Lenora Johnson, *Administrative Assistant*
Laura Kisthardt, *CLE Coordinator*

About the NSBA Council of School Attorneys
Formed in 1967, the NSBA Council of School Attorneys provides information and practical assistance to attorneys who represent public school districts. It offers legal education, specialized publications, and a forum for exchange of information, and it supports the legal advocacy efforts of the National School Boards Association.

Inquiry & Analysis is a membership service of the Council, or can be purchased by subscription for $180 per year. *Inquiry & Analysis* is published online ten times a year.

The articles in *Inquiry & Analysis* reflect the views and opinions of the individual authors, which do not necessarily represent the views and opinions of the National School Boards Association or The Council of School Attorneys. The views and opinions in the articles should not be relied upon and are not given for the purpose of providing legal advice.

National School Boards Association's Council of School Attorneys
1680 Duke Street, FL2
Alexandria, VA 22314-3493

Phone: 703.838.6722
Fax: 703.683.7590
E-mail: cosainfo@nsba.org
Web site: www.nsba.org/cosa
NSBA Connect: http://community.nsba.org

Copyright © 2016 by the National School Boards Association. All Rights Reserved.
ISSN: 2374-3956

National School Boards Association

cosa

Council of School Attorneys

Protecting Personal Information: Managing and Preventing Data Security Breaches

By Jill Greenfield, NSBA Legal Intern, National School Boards Association, Alexandria, Va

Data security breaches at companies across the country have become all too frequent and familiar. We remember when hackers gained access to over 70 million customer records by infecting Target's payment-card readers in 2013.[1] Before that, attackers stole information from more than 100 million accounts by infiltrating Sony's PlayStation Network in 2011.[2] These breaches are alarming because they leave us exposed to identity theft and fraud. But now, it's not just companies that are being hacked; schools and universities have increasingly become targets for these attacks, which leaves not just us, but also our students and school employees, vulnerable.

This article will discuss how data breaches can happen and what requirements exist under state law in case a breach does occur. Next, the article will address some ways school districts have handled recent security breaches. Finally, the article will suggest ways to prevent data breaches and protect personal information.

I. How Can Data Breaches Happen?

There are numerous ways an unauthorized person can acquire or gain access to personal information. Personal information, as the term is used in this article, is an individual's first and last name in combination with his or her social security number, driver's license number or state identification card number, or account number, credit, or debit card number with any code or password required for access to the individual's financial account. The most common methods of acquiring or accessing personal information are explained briefly below.

A. Malware/Virus

Malware, short for malicious software, is any software used to disrupt or gain access to computer systems or gather personal information. The best-known types of malware are viruses and worms, so named for the manner in which they spread (rather than for what they do to your computer). Malware is most commonly introduced when a user clicks on an infected advertisement, email, attachment, or website; computers that are not protected with anti-malware software are particularly vulnerable.

B. Hacking

The term "hacker" may conjure up the image of a pale adolescent feverishly typing away at a computer, but hackers come in all shapes and sizes and use a variety of techniques. Methods range from the high-tech—such as encryption-cracking tools, programs that capture keystrokes, or programs that monitor packets of information as they pass through a computer network—to the very low-tech, like impersonating IT employees or technical support personnel, sending phishing emails, or peeking through your garbage. The ultimate goal: to acquire user names, passwords, and credit card numbers the hackers can exploit.

C. Theft/Loss

Computers and laptops, portable electronic devices, and even paper files are susceptible to theft or loss. Laptops and thumb drives can contain a great deal of personal information, and this data becomes available to unauthorized individuals if the device is stolen or lost by a school district employee.

D. Unsecure Storage/Transmission

Unauthorized persons can acquire or gain access to personal information if it is sent or stored in

an unsecure place. For example, data can be intercepted in transit if it is emailed in plain text or sent in an unprotected attachment. Data is also at risk if files containing personal information are saved in a web folder that is publicly accessible online.

E. Unsecure Disposal

When computers reach the end of their usable life, they are either sold for reuse or disposed of. When those hard drives move on to their next destination, they may still contain personal information if they are not securely deleted or destroyed. An unauthorized person may even get personal information from paper records if they are discarded without first being shredded. Photocopiers are also an unexpected source of data because they may retain records of copies with personal information if their hard drives are not wiped before disposal.

F. Third-Party Contractors

School district employees are not the only ones with authorized access to personal information. Third-party contractors also access and possess school district data. This data can be vulnerable in the hands of that third party depending on the level of care the contractor uses. A contractor's servers may be infiltrated, personal information may be hacked in transit, or a physical device may be stolen while under the control of the contractor.

Recognizing the different ways an unauthorized person may acquire or gain access to personal information is critical in order to protect that sensitive data thoroughly. Section IV of this article provides suggestions for protecting personal information.

II. What Does State Law Require in the Case of a Breach?[3]

While the Family Educational Rights and Privacy Act (FERPA)[4], the Protection of Pupil Rights Amendment (PPRA)[5], and the Children's Online Privacy Protection Act (COPPA)[6] define a school district's responsibilities under federal law in the area of student data privacy,[7] much of a school district's obligations and potential liability for a data breach come from state law.

State law regarding data breaches varies widely, ranging from California, with extensive and detailed requirements, to Alabama, New Mexico, and South Dakota, all of which have no legislation regarding data breaches. The goal of this section is to provide a high-level overview of the current state legislation that applies to school districts. For more detailed guidance on the particular laws of your state, consult your COSA school attorney.

A. How Do States Define a Data Security Breach?

The Texas definition of a security breach is representative of a typical state law definition. A breach occurs if there is:

> Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.[8]

A majority of states use the term "unauthorized acquisition" of data to define a breach, but a sizable minority define a breach as access *and* acquisition of the relevant data. In a few states, access alone constitutes a breach, which means a breach can exist without actual procurement of the data by an unauthorized individual.

In addition to the exposure of the personal information, fifteen states also require that the unauthorized access and/or acquisition cause, or be reasonably likely to cause, harm in order to meet the definition of a breach.[9] This harm could take the form of economic loss, identity theft, or fraud, depending on the language of the statute.

Nearly all states have a good-faith employee acquisition exception. In these states, if an

employee or agent of the school district acquires personal information for a legitimate purpose and neither uses that information improperly nor makes further unauthorized disclosures of the information, that acquisition does not constitute a breach.

A majority of states also note that a breach has not occurred if data is secured by encryption or any other method that makes the personal information unreadable or unusable. Even in states whose statutes do not specifically name this exception, access and/or acquisition of encrypted data would likely not meet the definition of a breach as this would not compromise the security, confidentiality, or integrity of the personal information. If, however, an unauthorized individual is able to access or has acquired both encrypted data and the decryption key, a breach would result.

B. What Notification Requirements Exist?

The laws in most states that address the issue require school districts to notify affected individuals when a breach occurs. California's notification obligation is representative:

> Any agency [to which the statute applies] shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[10]

In most states, the notification requirement is triggered upon discovery or notification of a breach or when the entity becomes aware of a breach. About half of states, however, have an important exception to the notification requirement. Notice to affected individuals is not required if, after an appropriate investigation and consultation with law enforcement, the school district reasonably determines that no harm has or will likely result from the breach.

If notification is required, nearly all states stipulate that the disclosure be made "in the most expedient time possible and without unreasonable delay,"[11] but a few have more specific timing requirements. Almost all states, however, permit a delay of notification if a law enforcement agency determines that the notification will impede a criminal investigation.

Notice can generally be provided in written or electronic form; about half of states also permit telephonic notice. Different substitute notice mechanisms may be available if the breach affects a sufficiently large number of individuals or if notification will cost a sufficiently large sum of money.

A number of states' statutes enumerate the specific content the notice must include, but in general, the notice must be written in plain language and include when and how the breach occurred, what data was compromised, what the school district is doing to protect personal information from further unauthorized access, and contact information so that an affected individual can seek further assistance.

Finally, a majority of states have an exception that allows school districts to maintain their own notification procedures as part of an information security policy for personal information, provided that this policy is consistent with the timing requirements of the relevant state statute. If a district notifies affected individuals in accordance with its policies in the event of a breach, it is deemed in compliance with the state statute.

C. Who Else Needs to be Notified?

In addition to a notification obligation for affected individuals, some state statutes also require school districts to notify the state's Attorney General, specifically the Office of Consumer Protection (or some similarly-functioning agency), if a security breach should affect a certain number of people (commonly 500 or 1,000 individuals).

Many states also require that notice be provided to consumer reporting agencies in the event that more than a given number of individuals (commonly 1,000, but ranging from 500 to 10,000) are affected by a security breach. In these states, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis must be informed of the timing, distribution, and content of the notices.

D. How are These Laws Enforced?

In the majority of states, these laws are enforced by the state Attorney General, who is empowered to bring a civil action if a school district fails to comply with the state's statute. Some states permit the Attorney General to seek actual damages and/or injunctive relief in addition to civil penalties.

A minority of states have enumerated penalty structures in their statutes. They generally take the form of a maximum penalty per failure to notify (commonly $250 or $500, but as high as $10,000) along with a maximum penalty not to be exceeded for the entire security breach (commonly $150,000; ranging from $5,000 to $750,000).

Some states simply define a maximum penalty per security breach. Only Texas has established a minimum penalty ($2,000) along with a maximum ($5,000) per breach.[12] For a few states, such as Florida and Ohio, the magnitude of the penalty depends on the number of days the district is in violation.[13] Idaho and Michigan are the only states to have established criminal penalties for violations.[14]

Eleven states and the District of Columbia provide for a private right of action, allowing an individual injured by a breach or by failure to disclose a breach in a timely manner to bring a civil action for damages and/or injunctive relief.[15] The District of Columbia, for example, also permits residents to recover reasonable attorney's fees.[16]

With data security breaches becoming more and more common, state legislatures are continually modifying their laws. At least 25 states in 2016 have introduced or are considering security breach notification bills or resolutions.[17] This legislation could expand the definition of personal information, require businesses or government entities to implement security measures, and/or create additional requirements for educational institutions. With these changes on the horizon, consult your COSA school attorney to ensure your district is in full compliance with your state's current requirements.

III. What Have School Districts Actually Done When Breaches Occur?

With K-12 schools increasingly becoming targets of cyber-attacks, there is now a pool of experience to draw from should personal information be compromised in your district. In many cases, the way forward is clear: notify law enforcement and notify students, families, and employees. However, an increasingly popular type of attack, ransomware, is creating a difficult choice for school districts.

A. Ransomware: To Pay or Not to Pay?

In a ransomware (a type of malware) attack, a school district's data is encrypted by the attacker and taken hostage. The attacker will only provide the decryption key to make the data accessible again upon payment of a demanded sum of money, often in Bitcoin (a digital currency) because it is harder to trace. The question for school districts is whether to pay the ransom and get the district's data restored more quickly and get schools running normally, or to refuse and go through the time-consuming process of deleting the encrypted data and restoring that data from backup files.

The Horry County School District, the third largest school district in South Carolina, fell victim to a ransomware attack in 2016.[18] Up to 60% of the district's computers were frozen

within minutes and began to display a cryptic message that turned out to be a ransom note.[19] The district was forced to shut down more than 100 servers to stop the malware from spreading, but the district's data had become inaccessible.[20] Technology Director Charles Hucks made the decision to pay the ransom, about $10,000 in Bitcoin, in order to get the data back online faster and allow teachers and students to return to business as usual.[21]

In addition to being an expense school districts can ill afford, paying the ransom can be a risk. What if the ransom is paid but the attackers do not send the decryption key? Hucks wisely negotiated a "proof of life" type transaction to make sure the hackers delivered the key to avoid precisely this scenario. He also sent payment for just one machine first to make sure the decryption would work.[22]

Three other districts that faced a ransomware attack chose not to pay: the Swedesboro-Woolwich School District in New Jersey in 2015;[23] the North East Independent School District in Texas in 2016;[24] and the Cloquet School District in Georgia, also in 2016.[25] These districts suffered the inconvenience of operating without their computer systems while the encrypted data were deleted and restored from backup. This choice impacted teachers and students. Depending on the level of integration of technology, it can affect attendance systems, phones, and food service systems, among other aspects of the school day.

Refusing to pay the ransom is only an option, of course, if the school district has backup files from which to restore the data. Without these files, the only options are to lose the data entirely or to pay the ransom to get it back.

If faced with a ransomware attack, school districts should consider the following questions to determine whether to pay the ransom:

- How many schools or departments in the district are affected?
- To what degree does the lack of computers impact classroom operations and the schools' ability to function?
- How much money is the attacker asking for in ransom?
- How much data is affected?
- Are there backup files for the affected data?
- How long will it take to restore the system?

While districts will likely have to make individualized decisions, the FBI does not support or recommend paying a ransom in response to a ransomware attack because paying the ransom does not guarantee the organization will get its data back.[26] It also emboldens cyber criminals and incentivizes further criminal activity.[27] Instead, the FBI recommends prevention efforts and the creation of a business continuity plan should an attack occur.[28] Section IV below provides more information about prevention steps.

B. Making Students, Families, and Employees Whole Again: Providing a Credit Monitoring Service

Another question, should a breach occur, is what should school districts do to make students, families, and employees whole again? The exposure of a student's sensitive personal information can have long-term effects. A joint industry-academic study of 40,000 children caught up in a data breach found that someone else was using 10.2 percent of their social security numbers.[29] A student's social security number is uniquely valuable; it is unused, so it is a blank slate and can be paired with any name and birth date.[30] Additionally, the chance of discovery is low because the student will not be using the number for a long time and because parents usually do not monitor their student's identities.[31] The potential impact on the student's future is profound because identity theft can damage their ability to acquire a mobile phone,

get approval on a student loan, or obtain a job or a place to live.[32]

What can school districts do to mitigate the consequences of a breach? One step school districts can take is to provide credit monitoring and identity theft resolution services to families at no cost. For example, the Olympia School District in Washington is providing a two-year credit monitoring service to anyone affected by a recent data breach in 2016.[33] The program includes free credit reports, suspicious activity alerts, and identity theft insurance.[34] The district also provided staffed open computer labs to assist employees in signing up for these services, with times staggered to allow all types of employees to attend.[35]

The Katy Independent School District in Texas provided a similar proactive program to current and former employees affected by a 2015 breach.[36] The service was provided at no cost for three years.[37] Sequoia Union High School District in Oregon provided a service offered by one of the three U.S. credit reporting agencies at no cost for twelve months.[38] In the notice sent to affected individuals, the district also provided information on other steps to take, such as placing a Fraud Alert or a Security Freeze on their credit report, and/or obtaining a free credit report to monitor for fraudulent or irregular activity.[39]

Providing a credit monitoring service at no cost in the case of a breach is only required by law in a handful of states, but school districts can help minimize the damage and put families more at ease by making these services available.

IV. What Steps Can Be Taken to Prevent Data Breaches?[40]

Despite hackers' growing ability to infiltrate school districts' networks, there are numerous steps districts can take to make it harder for attackers to access and acquire personal information. The following are some best practices to consider to prevent data breaches.

A. Manage the Data and the Network

Know what data exists, what is being collected, and where it is stored. Only collect necessary personal information and be transparent with families about what data is collected and how it is used.[41] It is important to know what sensitive data the district maintains and where it is stored both in order to secure it and in order to inform affected individuals in the case of a breach.

Install a firewall, an intrusion detection/prevention system (IDPS), and anti-malware software. A firewall is designed to permit or deny network access based on a set of rules and is used to protect networks from unauthorized access, while still permitting legitimate access. An IDPS is a monitoring device that detects malicious activity on the network. Using a multi-layered defense reduces the risk of network infiltration.

Store and transmit data securely. Data that includes personal information stored on servers or on mobile devices should be encrypted. Any personal information being transmitted, particularly via email, should also either be redacted or encrypted. This can be done either by encrypting the data files or by encrypting the email transmissions themselves.

Control access to the data. Consider securing data access by requiring strong passwords and multiple levels of user authentication. Set limits on the duration of data access (e.g., locking access after the session times out) and limit administrator privileges. Determine which personnel within the district should have access to which categories of student and employee personal information. Place public access computers on a separate network to reduce the risk of an unauthorized person introducing a threat to the network that contains sensitive data.

Keep software up to date. "Patch management" is the process of regularly rolling out software updates and patches. A patch protects computers and applications by updating the security against

new threats or vulnerabilities. Develop a patch management plan to keep the system protected.

Delete data when it is no longer needed. Minimizing the amount of personal information being stored reduces the risk of exposure in case of hacking or theft. Deletions should only be made subject to the school district's or state's document retention schedule,[42] the Individuals with Disabilities Education Act (IDEA),[43] and other federal requirements.[44]

B. Educate Employees

Teach employees with access to personal information about the appropriate uses for that data. Create an acceptable use policy that outlines appropriate uses for the district's systems and incorporate security policies into employee responsibilities. Note that some states and federal grant programs require school districts to create such policies[45] and that state departments of education may provide guidelines, best practices, and/or sample considerations for the development of these policies.[46] Encourage employees to verify who has access to a given network location before saving, posting, or sending personal information.

Instruct employees to be cautious of suspicious advertisements, emails, attachments, and websites. Clicking on these unsafe links is the most common way malware is introduced; educating employees can help reduce this risk.

Encourage employees to use cryptic passwords and not to share them. Passwords that are difficult to guess are more secure. Initial and temporary passwords should be changed as soon as possible. Employees should use different passwords for work and non-work accounts.

C. Manage Physical Devices and Physical Access

Inventory and secure portable devices. Laptops should be kept in sight or locked to a work station or other secure location. To avoid theft, papers, computers, and other electronic devices should not be left visible in an empty car or house. Consider extra security measures like encryption for portable devices. Also, be sure to monitor inexpensive assets like thumb drives that can contain valuable personal information.

If your district has a "Bring Your Own Device" (BYOD) program, establish security policies. Each device can introduce threats when connected to the network, so create a list of approved devices and a strategy for securing them.[47]

Destroy or securely delete data before re-using or disposing of equipment. Securely erase printers, fax machines, and photocopiers before resale, disposal, or returning them to the vendor, again in accordance with relevant document retention schedules and federal regulations. Shred paper records with personal information before disposing of them.

Restrict physical access to areas where personal information is stored. Secure access to any areas where sensitive data is stored, such as buildings and server rooms. Consider locking office doors, installing card access control to buildings or offices, locking file cabinets, and having auto log off functionality on computers.

D. Manage Third Parties

Do the due diligence. Interview vendors and review their security policies regarding employee background screening and data management. Examine the vendor's insurance coverage and any prior legal complaints, litigation, or regulatory actions in this area with the assistance of your COSA school attorney.

Know which online educational services are being used in your district. Today's classrooms increasingly use computer software, mobile applications (apps), and web-based tools provided by third parties that may use student information. Have policies and procedures to evaluate and approve proposed online educational services.[48]

Draft data security contract language. Work with your COSA school attorney to specify how the data should be handled while it is in use and how it will be returned or erased. Be sure the contractor has read and understood any data security contract provisions.

De-identify the information that goes to vendors. Remove personal information as much as possible from any data that gets sent out to third-party contractors to reduce the risk of exposure.

E. Create a Response Plan[49]

Typically, school districts already have crisis management plans in place for instances of school violence and weather issues, among other emergency situations. Establishing a similar type of plan for responding to a data breach will promote better response coordination and will help school districts respond more quickly. A prompt response reduces the risk of further data loss and can mitigate any negative consequences of the breach, including potential harm to students and employees. Efficient incident handling will also help reduce a district's liability associated with delayed reporting and notification.

The Privacy Technical Assistance Center (PTAC), established by the U.S. Department of Education, has created a checklist designed to illustrate some current best practices in data breach response and mitigation.[50] Though the checklist may not be exhaustive, it is an excellent starting point for school districts to create their own individually tailored response plans. In creating the plan for your district, consult your COSA school attorney for further guidance.

With hackers increasingly targeting schools and with data breaches on the rise, school districts should take steps to protect their networks and personal information to prevent a breach, be prepared to respond to a breach, and be informed about the requirements under both state and federal law should a breach occur. It is not so much a matter of if, but when an attack will happen. It is imperative for districts to start the conversation about data security now in order to implement the necessary technologies and practices to mitigate the effects of a breach before it happens.

---

[1] Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. TIMES, Jan. 10, 2014, http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html.
[2] Nick Bilton, *Sony Explains PlayStation Attack to Congress*, N.Y. TIMES: BITS (May 4, 2011, 12:59 PM), http://bits.blogs.nytimes.com/2011/05/04/sony-responds-to-lawmakers-citing-large-scale-cyberattack/.
[3] Perkins Coie Privacy & Sec. Grp., *Security Breach Notification Chart* (revised June 2016), https://dpntax5jbd3l.cloudfront.net/images/content/1/5/v2/157234/Security-Breach-Notification-Law-Chart-June-2016.pdf (last visited July 13, 2016).
[4] 20 U.S.C. § 1232g.
[5] 20 U.S.C. § 1232h.
[6] 15 U.S.C. §§ 6501 *et seq.*
[7] For more information, see NSBA COUNCIL OF SCH. ATTORNEYS, DATA IN THE CLOUD: A LEGAL AND POLICY GUIDE FOR SCHOOL BOARDS ON STUDENT DATA PRIVACY IN THE CLOUD COMPUTING ERA (Apr. 25, 2014), *available at* www.nsba.org/data-cloud; *see also* NSBA COUNCIL OF SCH. ATTORNEYS, CLOUD COMPUTING AND STUDENT PRIVACY: A GUIDE FOR SCHOOL ATTORNEYS (May 30, 2014), *available at* www.nsba.org/cloud-computing-and-student-privacy-guide-school-attorneys (access restricted to attorney members of NSBA's Council of School Attorneys).
[8] TEX. BUS. & COM. CODE § 521.053(a).
[9] Arizona, Hawaii, Kansas, Massachusetts, Montana, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Utah, Virginia, West Virginia, and Wyoming.

[10] CAL. CIV. CODE § 1798.29(a).
[11] *E.g.*, N.Y. GEN. BUS. LAW § 899-aa(2).
[12] TEX. BUS. & COM. CODE § 521.151(a).
[13] FLA. STAT. § 501.171(9)(b); OHIO REV. CODE ANN. § 1349.192(A)(1).
[14] IDAHO CODE ANN. § 28-51-105(1); MICH. COMP. LAWS § 445.72(12).
[15] Alaska, California, Louisiana, Maryland, Minnesota, Nevada, New Hampshire, North Carolina, South Carolina, Tennessee, and Washington.
[16] D.C. CODE § 28-3853(a).
[17] Nat'l Conference of State Legislatures, *2016 Security Breach Legislation* (May 3, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/2016-security-breach-legislation.aspx.
[18] Jonathan Levine, *Preparing Schools for Ransomware – the Next Big Threat to Education*, EDSURGE (June 11, 2016), https://www.edsurge.com/news/2016-06-11-preparing-schools-for-ransomware-the-next-big-threat-to-education.
[19] David Fitzpatrick & Drew Griffin, *'Ransomware' Crime Wave Growing*, CNN MONEY (Apr. 4, 2016, 6:14 PM), http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime.
[20] Levine, *supra* note 18.
[21] Fitzpatrick & Griffin, *supra* note 19.
[22] *Id.*
[23] Walt Hunter, *Computer System Network for Swedesboro-Woolwich School District Hacked*, CBS PHILLY (Mar. 24, 2015, 3:13 PM), http://philadelphia.cbslocal.com/2015/03/24/computer-system-network-for-swedesboro-woolwich-school-district-hacked/.
[24] Jeremy Baker, *Ransomware Attacks 20 North East ISD Schools*, KENS5 EYEWITNESS NEWS (Apr. 7, 2016, 10:10 PM), http://www.kens5.com/news/education/in-our-schools/ransomware-attacks-20-northeast-isd-schools/125053680.
[25] Jana Hollingsworth, *Cloquet Schools Suffer 'Ransomware' Attack*, DULUTH NEWS TRIBUNE (Mar. 17, 2016, 5:30 PM), http://www.duluthnewstribune.com/news/crime/3989320-cloquet-schools-suffer-ransomware-attack.
[26] *Incidents of Ransomware on the Rise: Protect Yourself and Your Organization*, FBI (Apr. 29, 2016), https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise.
[27] *Id.*
[28] *Id.*
[29] Ron Lieber, *Identity Theft Poses Extra Troubles for Children*, N.Y. TIMES, Apr. 17, 2015, http://www.nytimes.com/2015/04/18/your-money/a-childs-vulnerability-to-identity-theft.html?_r=0.
[30] RICHARD POWER, CARNEGIE MELLON CYLAB, CHILD IDENTITY THEFT: NEW EVIDENCE INDICATES IDENTITY THIEVES ARE TARGETING CHILDREN FOR UNUSED SOCIAL SECURITY NUMBERS (2011), https://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf.
[31] *Id.*
[32] *Id.*
[33] Lisa Pemberton, *Olympia School District Data Breach Affected 90 Student Workers*, THE OLYMPIAN (May 3, 2016, 4:22 PM), http://www.theolympian.com/news/local/education/article75344167.html; *see also* COMMUNICATIONS DEP'T, OLYMPIA SCH. DIST., OSD DATA BREACH (APRIL 12) – STAFF INFORMATION, http://osd.wednet.edu/news/osd_data_breach_-_staff_information (last updated May 25, 2016).
[34] Pemberton, *supra* note 33.
[35] *Id.*

[36] Sebastian Herrera, *Katy ISD Offers Credit Monitoring to Current, Past Employees amid Possible Breach*, HOUSTON CHRONICLE (Aug. 19, 2015, 3:09 PM), http://www.houstonchronicle.com/neighborhood/katy/schools/article/Katy-ISD-offers-credit-monitoring-to-current-6451816.php (full article available to subscribers of the Houston Chronicle).
[37] *Id.*
[38] Dr. James Lianides, Superintendent, Sequoia Union High Sch. Dist., *Notice of Data Breach*, https://oag.ca.gov/system/files/Sequoia%20-%20CA%20Notice%20(6003570x7AB84)_1.pdf.
[39] *Id.*
[40] Univ. of Cal. Santa Cruz Info. Tech. Servs., *Security Breach Examples and Practices to Avoid Them*, http://its.ucsc.edu/security/breaches.html (last visited June 29, 2016); U.S. DEP'T OF EDUC. PRIVACY TECH. ASSISTANCE CTR., DATA SECURITY CHECKLIST (revised July 2015), *available at* http://ptac.ed.gov/sites/default/files/Data%20Security%20Checklist.pdf; Ronald C. Wanglin, Bolton & Co., *Managing the Risk of Data Breach*, http://www.boltonco.com/industryexpertise/managingtheriskofdatabreach (last visited June 29, 2016).
[41] For more information, see U.S. DEP'T OF EDUC. PRIVACY TECH. ASSISTANCE CTR., TRANSPARENCY BEST PRACTICES FOR SCHOOLS AND DISTRICTS (July 2014), *available at* http://ptac.ed.gov/sites/default/files/LEA%20Transparency%20Best%20Practices%20final.pdf.
[42] *See, e.g.*, VA. CODE ANN. § 42.1-85 (authority to develop regulations governing retention and disposition of state and local public records); Library of Virginia, *Records Retention and Disposition Schedule, General Schedule No. GS-21: County and Municipal Governments – Public School* (May 6, 2016), *available at* http://www.lva.virginia.gov/agencies/records/sched_local/GS-21.pdf.
[43] *See* 20 U.S.C. § 1417(c); 34 C.F.R. § 300.624 (2015).
[44] *See* U.S. DEP'T OF EDUC. PRIVACY TECH. ASSISTANCE CTR., BEST PRACTICES FOR DATA DESTRUCTION (May 2014), *available at* http://ptac.aem-tx.com/sites/default/files/Best%20Practices%20for%20Data%20Destruction%20%282014-05-06%29%20%5BFinal%5D.pdf.
[45] *See, e.g.*, VA. CODE ANN. § 22.1-70.2; *see also* PRINCE WILLIAM CNTY. PUB. SCH., RESPONSIBLE USE AND INTERNET SAFETY POLICY (Oct. 22, 2014), *available at* http://pwcs.edu/UserFiles/Servers/Server_340140/File/Migration/Policies%20&%20Regulations/Internet%20Privacy%20Policy/R295-1.pdf (example of Virginia school district acceptable use policy).
[46] *See, e.g.*, OFFICE OF KNOWLEDGE, INFO. AND DATA SERVS., KY. DEP'T OF EDUC., GUIDELINES FOR CREATING ACCEPTABLE USE POLICIES (July 17, 2013, 1:40 PM), http://education.ky.gov/districts/tech/Pages/Acceptable-Use.aspx.
[47] For more information, see *Avoiding a Data Breach: Cybersecurity at K-12 Institutions*, Plante Moran (Dec. 3, 2015), http://www.plantemoran.com/perspectives/articles/2015/pages/avoiding-a-data-breach-cybersecurity-at-k12-institutions.aspx (excerpt from "The Technology Imperative: Staying Ahead of the Curve in the Classroom").
[48] For more information, see U.S. DEP'T OF EDUC. PRIVACY TECH. ASSISTANCE CTR., PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: REQUIREMENTS AND BEST PRACTICES (Feb. 2014), *available at* http://ptac.aem-tx.com/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf; *see also* U.S. DEP'T OF EDUC. PRIVACY TECH. ASSISTANCE CTR., PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: MODEL TERMS OF SERVICE (revised Mar. 2016), *available at* http://ptac.ed.gov/sites/default/files/TOS_Guidance_Mar2016.pdf.
[49] U.S. DEP'T OF EDUC. PRIVACY TECH. ASSISTANCE CTR., DATA BREACH RESPONSE CHECKLIST (Sept. 2012), *available at* http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf.
[50] *Id.*