NAIS LEGAL ADVISORY

Cybersecurity in Independent Schools: Data Breach Threats and Prevention Techniques

Whitney Silverman, NAIS Staff Attorney, silverman@nais.org
December 2018

These days it seems that major companies announce significant breaches of their customers' personal information with alarming frequency. If large companies are so vulnerable, what are nonprofits such as independent schools to do to protect the personal and sensitive information of students, staff, and donors? Similar to other risk management efforts, a focus on prevention as well as readiness to respond to a crisis is key. This advisory provides an overview of the cybersecurity landscape and top threats, the legal landscape and liability concerns, and tips to shore up cybersecurity and privacy protections in independent schools.

Cybersecurity and Incident Landscape

A cybersecurity incident brings reputational, financial, and legal risks and can touch any educational institution, from a small independent school to a metropolitan school district to a large university system. In fact, each incident described in this advisory has happened to a school in one fashion or another over the past few years. According to the Privacy Rights Clearinghouse, over the past five years (2014-2018), the education sector has experienced 140 publicly known breaches affecting 51,101,763 records. Hacking or malware incidents were the most common, followed by unintended disclosure such as unintended publishing or sending of information, device or physical data loss—either through theft or accidental misplacement, and intentional misappropriation of information by insiders such as employees.[1] This data is mirrored by the larger picture. A 2018 study from Verizon shows that 75

[1] *Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breaches?title=&org_type%5B%5D=259&taxonomy_vocabulary_11_tid%5B%5D=2436&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473 (last visited Nov. 14, 2018).

percent of data breaches are caused by external attackers while a combination of accidental, negligent, and intentional harmful activity by insiders accounts for the rest. According to Verizon, the picture in the educational sector is even more acute with 81 percent of attacks being brought about by external parties, with social engineering schemes emerging as a top concern.

One type of hacking/malware risk is phishing or social engineering attacks, where bad actors pose as a known person or organization and use email or websites to obtain personal information and access. Often, the message or website looks legitimate, but something such as spelling, grammar, url, or the logo may be slightly off. For example, the human resources director receives an email from the "Head of School" asking for copies of all employee W-2 forms to be sent over ASAP. Without looking to realize that the school email address ending is spelled incorrectly, they respond to the email with the W-2 forms, the hacker files false tax returns and fraudulently obtains refunds, and other information such as date of birth, address, and social security number are exposed. Over the past few years, the IRS has raised the alarm that these W-2 scams are on the rise, with a particular warning to schools and nonprofits.[2]

Vendor relationships are another risk point. In this case, the business officer receives an email from a "vendor" saying that the next payment is due, and the banking information has changed. The business officer clicks on the link and routes the payment to the provided bank account and the school is now out thousands of dollars. Additionally, hackers may attempt to take advantage of routine staff update emails. In this instance, the staff all receive a notice from "IT" that it is time to change their passwords. Some staff click on the provided link and the hacker now has their login credentials and access to sensitive student and staff information. Last, students, including international students for whom English is not their first language, can be at risk for a variety of email-based scams peddling false admissions offers and/or the need to make payments immediately to a new account.[3]

Another worrying hacking trend in the use of ransomware. According to the 2017 Cost of Cyber Crime Study, ransomware is on the rise. In 2016 it composed 13 percent of cyberattacks and by 2017 that

[2] Press Release, IRS, Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others (Feb. 2, 2017), https://www.irs.gov/newsroom/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others.
[3] *See Protecting Yourself from Scams*, UC Davis, https://siss.ucdavis.edu/scams.

percentage doubled, with ransomware attacks at 27 percent.[4] In this circumstance, the head of school arrives Monday morning to a worrying message—a hacker has locked everyone out of the school's systems and is holding the data hostage. If the school pays a ransom, access will be restored. If not, personal information of students and staff will be released online. A group called "Dark Overlord" has being doing this to schools across the country in recent months. In some troubling instances, members of the school community who were hacked even received text messages from the hackers threatening bodily harm.[5]

Additionally, human error can result in accidental, but consequential, data loss events. It is common for employees to take their work devices home and a laptop that is left in an Uber or stolen[6] on a train can place sensitive information at risk, particularly if it is not encrypted. Additionally, an employee can inadvertently attach a document to an email or social media post and send personal information to an audience beyond those authorized to see it. Technical and system updates are also a point of risk. For example, an error made when transitioning to a new server can leave a school's system exposed, with community members able to access records that should be restricted to particular users.[7]

Last, the combination of a hacker and lax digital hygiene can combine for problematic results. Schools collect and retain large amounts of data and documents from current students and staff, parents, applicants, donors, vendors, and others. Occasionally, too much data is requested—perhaps the school collects Social Security numbers when it is not necessary to do so—or records are kept for years on end, seemingly in perpetuity. The school does not perform regular IT system scans and has not implemented certain security practices like encryption or multifactor authentication to access sensitive information.

---

[4] PONEMON INST. & ACCENTURE, 2017 COST OF CYBER CRIME STUDY 23 (2017), *available at* *https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50*.

[5] *See* Valerie Strauss and Moriah Balingit, *Education Department warns of new hacker threat as 'Dark Overlord' claims credit for attacks on school districts*, WASHINGTON POST (Oct. 26, 2017), https://www.washingtonpost.com/news/answer-sheet/wp/2017/10/26/education-department-warns-of-new-hacker-threat-as-dark-overlord-claims-credit-for-attacks-on-school-districts/?utm_term=.20beb7bb8ef5.

[6] *See* Letter from UC Santa Cruz, Notice of Data Breach, https://oag.ca.gov/system/files/UCSC_Notification_Letter_2017-01_0.pdf.

[7] *See* Dana Branham, OU Shuts Down File Sharing Service After Failing to Protect Thousands of Students' Records, OU DAILY (June 13, 2017), http://www.oudaily.com/news/ou-shuts-down-file-sharing-service-after-failing-to-protect/article_4f9a5e2c-50a2-11e7-a807-2f591e6c54f0.html.

Eventually, a data breach is discovered and the data of thousands of current and past community members—as well as applicants who never attended the school—is at risk.[8]

The Legal Landscape

Currently there is not a uniform standard for all data security and breach response protocols, although some momentum is building in that direction.[9] On the federal level, the United States takes a sector-specific approach (e.g., health care information is covered by HIPAA, education information for schools who take federal funds is covered by FERPA, the information of children online is protected by COPPA, and financial information is covered by various laws including Gramm-Leach-Bliley and the FTC Red Flags rule).[10] If an independent school holds data covered by a sector-specific federal law such as FERPA or HIPAA, those rules and obligations will apply. Schools may also be affected by international laws when they hold the data of residents from other countries. For example, if you have data from a resident of the European Union, the General Data Protection Regulation (GDPR) may kick in.[11]

However, it is more likely that a state law governing security and/or data breach response applies to your school. As of October 2018, at least 22 states have laws requiring businesses to maintain a base level of security.[12] While these laws differ, they generally require implementing and maintaining security protocols that are reasonable based on the organization's size and the sensitivity of the data it holds.

---

[8] *See* Victoria Sundqvist, *Yale University Sued Over 2008 data breach*, NEW HAVEN REGISTER (Oct. 17, 2018), https://www.nhregister.com/news/article/Yale-University-sued-over-2008-data-breach-13315315.php.

[9] *See* Ryan Chiavetta, *Intel Launches Online Portal for Consultation on its US Federal Privacy Law* (Nov. 8, 2018), https://iapp.org.

[10] See other NAIS Advisories such as "Seven Steps to Address Your School's Privacy Obligations" by Bret Cohen, Stephanie Gold and Debra Wilson (June 2010), https://www.nais.org/articles/pages/member/seven-steps-to-address-your-school-s-privacy-oblig/, "Protecting Student Privacy While Using New Technologies and Collecting Student Data," by Valerie Brennan and Michelle Tellock (2017), https://www.nais.org/articles/pages/member/protecting-student-privacy/, and "Technology in the Classroom: Is Your School in Compliance" by Hogan Lovells LLP (2013), https://www.nais.org/Articles/Documents/Member/TechInClassroom.pdf, for further information on these other privacy laws.

[11] *See* Debra P. Wilson and Whitney Silverman, *General Data Protection Regulation and Independent Schools* (Mar. 2018), https://www.nais.org/articles/pages/member/nais-legal-advisory-general-data-protection-regulation-and-independent-schools/.

[12] *See* Data Security Laws Private Sector, NAT'L CONFERENCE OF STATE LEGISLATURES (Oct. 15, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

Additionally, all 50 states now have laws covering data breaches.[13] Depending on the nature of the breach, you may have to notify the state attorney general, a regulatory body, and/or the individuals affected. You may also be required, or consider providing, information on fraud alerts, credit freezes, and a period of free identify-theft protection services to affected persons.

These laws can be seen as establishing a standard of care. Recent lawsuits against educational institutions cite these laws as a basis for a litany of claims such as negligence and unfair trade practices.[14] Meanwhile, other lawsuits involving data breaches and identity theft have claimed emotional distress, invasion of privacy, and breach of contract, amongst other causes of action.[15] These lawsuits are not always successful, but can take years to move through the system and be costly, both to the pocketbook and to an organization's reputation. Understanding your state's requirements and implementing appropriate safeguards can help minimize risk and the lower the chance of liability in a government enforcement action or a private lawsuit. At least one state recently passed a law that provides a safe harbor and affirmative defense—a shield against liability—if they have, maintain, and follow the cybersecurity requirements outlined under the law.[16] We may see more states move in that direction to encourage more robust, preventative cybersecurity programs.

Prevention and Response

Increasingly, companies have come to understand the value of prevention efforts and are spending more money on preventative activities such as cybercrime detection and containment.[17] However, a striking number of organizations do not have a cybersecurity incident response plan. There are many steps independent schools can take to improve their prevention posture, decrease the likelihood of an attack, and limit the damage if one occurs.

- **Pull together your team.** For many schools, the first step will be to take an inventory of the types of data or personal information the school collects, from whom it is collected, where it is

[13] *See Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[14] *See* Victoria Sundqvist, *Yale University Sued Over 2008 data breach*, NEW HAVEN REGISTER (Oct. 17, 2018, 4:12 PM), https://www.nhregister.com/news/article/Yale-University-sued-over-2008-data-breach-13315315.php.
[15] *See* Sackin v. Transperfect Global, Inc., 278 F. Supp. 3d 739 (S.D.N.Y. 2017); Ree v. Zappos.com, Inc. (In re Zappos.com, Inc.), 888 F.3d 1020 (9th Cir. 2018).
[16] Ohio Rev. Stat. § 1354.01-1354.05.
[17] Cost of Cyber Crime Study at 30.

stored, and how it is protected. To get an accurate and comprehensive picture, getting the right people involved in the conversation is key, and likely will include senior leadership and IT as well as personnel from human resources, business office, admissions, advancement, and financial aid.

- **Evaluate the weak points and risks in your IT system.** What are your greatest risks for data breach or loss? Under what scenarios could breach or loss occur? Do you currently utilize data minimization principles[18] and follow a document retention schedule?[19] Schools should think beyond technology-related threats to include natural disasters, terrorist attacks, fire, and other structural damage. Incorporate plans for mitigating, monitoring, and continually evaluating those risks in your data privacy and security and continuity of operations plans.
- **Determine what types of data protections—both technological and process-related—you can implement in the near and long term and train your staff accordingly.** The type of data protections your school needs (administrative, technical, and physical) will depend and vary based on the size of your school and the types of information you maintain. The manner and frequency of training—be it in-person table-top exercises, online modules, or even (somewhat controversial) phishing simulation tests[20]—will also depend on those factors. The Association of Technology Leaders in Independent Schools' recent cybersecurity report has three levels of steps schools can take depending on their baseline, needs, and capacity. [21]
- **Take stock of your vendor agreements and have a process to help teachers (and administrators) evaluate new applications or education technology services to protect your data**. Schools, like many organizations, often outsource aspects of their technical operations and use vendors for everything from student and staff applications, learning management systems, tuition payments, and more. It is important to evaluate these agreements for privacy, data minimization, data destruction, and data protection provisions, as well as allocation of responsibility and liability in the case of a data breach. Additionally, educators are often

[18] *See Best Practices for Data Destruction*, U.S. DEPT. OF EDUC., https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282014-05-06%29%20%5BFinal%5D_0.pdf.
[19] *See* Debra P. Wilson and Whitney Silverman, *Records Retention: What, How Long, and How?* (June 2018), https://www.nais.org/media/MemberDocuments/Legal/NAIS_Legal_Advisory_Records_Retention_2018-7-3-2018.pdf.
[20] Marika Samarati, *Infographic: Phish Your Staff Before Cyber Criminals Do*, IT GOVERNANCE (Sept. 12, 2016), https://www.itgovernance.co.uk/blog/infographic-phish-your-staff-before-cyber-criminals-do.
[21] ASS'N OF TECH. LEADERS IN INDEP. SCH., CYBERSECURITY RECOMMENDATIONS FOR INDEPENDENT SCHOOLS (2018), *available at* https://www.theatlis.org/assets/docs/ATLIS_Cybersecurity_Recommendations2018.pdf.

interested in introducing new apps or programs into their classroom. Often, these come with take-it-or-leave-it "click wrap" agreements. Ideally, schools should have a process for reviewing and tracking the use of new ed tech across the board.[22]

- **Evaluate your insurance coverage.** As cyberattacks and data breaches are becoming more common, it is critical to understand what your current insurance policy covers and if additional cyber liability coverage is necessary. In some recent cases, insurance companies have pushed back when companies who suffered social engineering phishing attacks tried to invoke their existing business insurance policies' computer fraud provisions. Although the companies ultimately prevailed,[23] this area of insurance is rapidly changing and is not necessarily keeping up with technological advances.
- **Be aware of common cyber threats that may be trending throughout the country, including W-2 scams and cyber-extortion schemes.** The FBI, IRS and federal Department of Education—as well as state Departments of Education and Attorneys General—will often provide alerts and updates on these threats, how to avoid them, and how to report an incident if one should occur.
- **Response.** If you believe you have experienced a data loss or breach, you should bring together your team to answer the following questions:
    - Did a breach actually occur? Obtain information to validate whether a breach has actually occurred and get a sense of the initial scope. Be sure to document all efforts at this and later investigatory stages.
    - What type of investigation is needed? When you suspect or know a breach has occurred, an investigation of some sort should follow. Depending on the scope, you may want to notify your counsel. Your attorney can help guide you in the investigation and provide attorney-client privilege for that investigation (and potentially the activities of any hired third-party forensic investigators) to the extent allowable.
    - How will you communicate? Outside of required notifications to regulatory authorities and/or affected persons, think about how you will communicate the breach to your

[22] *See Protecting Student Privacy While Using Online Educational Services: Model Terms of Service*, U.S. DEP'T OF EDUC (Jan. 2015), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Jan%202015_0%20(1).pdf.

[23] *See* Medidata Sols. Inc. v. Fed. Ins. Co., 729 Fed. Appx. 117 (2d Cir. 2018); Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455 (6th Cir. 2018).

broader community, particularly if the incident is widespread, and how will you respond to media requests.

- How will you move forward and build in the lessons from your experience? Evaluate your data breach response plan and note what worked well and what can be improved. Additionally, outline and implement new security procedures that could mitigate or thwart the risk of similar loss or breach in the future.

Conclusion

Cybersecurity has made it to the top of many risk assessment lists and awareness continues to grow. Although the federal government hasn't passed comprehensive privacy and data-breach standards, states continue to enhance security and breach-notification requirements. With these guidelines and recommendations from federal agencies and nonprofits, independent schools can make important strides in this arena while continuing to innovate in teaching and learning.

Resources

- Verizon 2018 Data Breach Investigations Report
- K-12 Cybersecurity Resource Center
- Association of Technology Leaders in Independent Schools Cybersecurity Recommendations
- Readiness and Emergency Management for Schools (REMS) Technical Assistance Center: Cybersecurity Considerations for K-12 Schools and School Districts
- U.S. Department of Education Data Security: Top Threats to Data Protection
- U.S. Department of Education: Data Breach Response Training Kit
- Federal Trade Commission Cybersecurity for Small Business
- National Council of Nonprofits: Feeling Insecure About Security?
- NAIS: Seven Steps to Address Your School's Privacy Obligations
- NAIS: Protecting Student Privacy While Using New Technologies and Collecting Student Data
- NAIS and ATLIS: Understanding and Managing Issues in School, Technology, Data, and Privacy
- NAIS: Crisis Communications Guidelines for Independent Schools
- NAIS and United Educators: Advancing Risk Management at Independent Schools

This information is provided for educational purposes only. Schools should work with legal and tax counsel to ensure proper compliance with tax and other laws.