CARLTON FIELDS

Cybersecurity Obligations and Best Practices for Independent Schools

CYBERSECURITY AND PRIVACY | EDUCATION | MARCH 15, 2019


Michael L. Yaeger


John E. Clabby


James M. Sconzo


Joseph W. Swanson

Independent schools, like other non-profits, have valuable digital assets that bring cybersecurity obligations with them. For example, schools typically extend financial aid to students and medical benefits to employees only after collecting sensitive personal information. That kind of data is protected in all 50 states and the District of Columbia by breach notification laws. [1] Further, much of the data that schools possess is the personal information of minors, which brings with it a host of additional sensitivities. In this article, we provide an overview of independent schools' legal obligations and then provide some best practices to help schools meet those obligations and manage risk.

Legal Obligations

State breach notification laws claim to follow state residents' data wherever it goes. A school that educates students or employs teachers who reside in New York, New Jersey, and Connecticut, for example, may have notification obligations in all three states.[2]

And many states, including California, Connecticut, Maine, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, and Rhode Island, require that an entity in possession of "personal information" notify affected individuals after that information is breached if the entity reasonably believes[3] that unencrypted personal information[4] was "accessed" or "acquired by"[5] an unauthorized person.[6] Some states qualify the rule by adding a harm analysis. Rhode Island, for example, does not require disclosure unless the breach "poses a significant risk of identity theft."[7] But in most states the harm analysis is less forgiving, and California and New York do not predicate notification on a harm analysis. Further, all nine of the above-mentioned states impose civil penalties for not complying with their data breach notification law that can be enforced by the state Attorney General or, in California, New Hampshire and possibly New Jersey, [8] by a private party in a lawsuit.

Independent schools also face potential liability under consumer protection laws, as well as common law liability for negligence. If a school promises students or employees that their personal information would not be disclosed to third parties without their consent, a school might take on a legally enforceable duty of care. In addition, parents might allege that a school's failure to properly secure personal information resulted in a breach of fiduciary duty. And if a student can allege that a third party stole her personal information from the school and used the information to her detriment – by, for example, opening fraudulent credit card accounts and making fraudulent purchases – then the student may have a claim that could survive a motion to dismiss.[9] In effect, the possibility of negligence liability may create an obligation to take reasonable cybersecurity measures.

California**,** Connecticut, Massachusetts, and Rhode Island also create compliance obligations more directly by requiring the adoption of information security programs.[10] Connecticut, for example, requires the ["safeguard[ing]" of personal information from "misuse by third parties," and the adoption of a "privacy protection policy" by "[a]ny person who collects Social Security numbers in the course of business."][11]

For certain private schools, and in particular private boarding schools, the European Union's new General Data Protection Regulation (GDPR) may also be relevant. In general terms, the GDPR governs those entities, including U.S. entities, that

collect or process data of European residents. While there is much more to it than that, U.S.-based boarding schools that advertise to European applicants, bill or send invoices to parents at an address in Europe, or track alumni who are living in Europe for development purposes, should consider whether the GDPR applies to their operations.

However, independent schools do catch one break. Most public schools are subject to the Family Educational Rights and Privacy Act (FERPA), [12] which provides certain privacy protections for students' education records and prohibits the improper disclosure of personal information derived from education records. Independent schools — provided that they do not receive funding from the U.S. Department of Education — are not subject to FERPA.

Best Practices

Developing a formal program with written policies

- As part of their efforts to satisfy these obligations, schools should develop both written information security plans (sometimes called WISPs) and written incident response plans.
    - A WISP provides a general overview of the information security measures currently in place at your firm. These include physical, administrative, and technical security controls.
    - An incident response plan is more like an order of operations to follow during an incident.
- Before developing policies, schools may be well-served by engaging an outside consultant to conduct a risk assessment that informs the drafting.
- Schools should be wary of wholesale adoption of an outside consultant's form policy, as it may not be sufficiently tailored to the school's particular risks. A good policy is one that is drafted in collaboration with IT staff and others who actually have to carry it out.

Conducting regular risk assessments

Schools should consider conducting regular reviews to reassess cybersecurity risks. As the saying goes, "security is a process, not a product."[13] Policies and procedures should not just be established, but periodically revisited and reconsidered.

- After a risk assessment, identified threats and vulnerabilities should be matched to specific policy elements.
    - Consider starting this process in a chronological order, starting with admissions, moving through students' records (including billing and medical information), and ending with consideration of how alumni and development records are kept.

Managing vendor risk

- A good portion of a school's important data may actually be in the possession of its vendors, such as the companies that process financial aid applications and payroll. Schools should conduct due diligence of vendors when they are selected, including assessment of a vendor's creditworthiness when the vendor is not a household name, and negotiate cybersecurity protections into contracts.
- The vendor should identify any subcontractors that will have access to sensitive information and should provide diligence material for each subcontractor.

Providing oversight

- Senior leadership and a school's Board should be engaged in the security process, both by approving policies and by receiving regular updates on cybersecurity risk and more significant incidents or suspected or actual data loss.
- The Board should review annual budgets to ensure sufficient funding for privacy and security, assign roles and responsibilities, and get regular briefings on cyber issues.
- The Board cannot and should not be involved in managing risks on a day-to-day basis, but should instead focus on setting up systems and ensuring that they are resilient in the face of incidents such as an attack or a vendor's failure.

Training personnel

Some of the most likely risks, such as malware infections from email phishing attacks, can be lowered by training employees. Moreover, training employees is a useful protection against certain negligence arguments that could arise in litigation.

- Compliance tip: When you are training employees to recognize phishing attacks, also train them to report even unsuccessful attacks so that later attacks from the same source can be blocked.

Conclusion

Given the data that independent schools possess and the exposure and reputational harm that would flow from a breach, these organizations must manage cybersecurity risk like other enterprise-wide perils. Implementing the best practices identified above should be a priority for these schools.

---

[1] *See* Nat'l Conf. of State Legislatures, Security Breach Notification Laws, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Jan. 21, 2019). Guam, Puerto Rico and the Virgin Islands also have data breach notification laws.

[2] *See* Conn. Gen Stat. § 36a-701b; N.J. Stat. § 56:161 through 56:166 ; N.Y. Gen. Bus. L. § 899-aa2 and 399-h.

[3] Or "has reason to know." *See* Mass. Gen. Laws § 93H-3(b).

[4] In all of these states encryption is a safe harbor, but the structure of the statutes is different. California, Connecticut, Massachusetts, New Jersey, and Pennsylvania place the safe harbor in the definition of "breach of security." That is, they define a breach to exclude personal information that has been encrypted. *See* Conn. Gen Stat. § 36a-701b(a); Mass. Gen. Laws § 93H-3(a); N.J. Stat. § 56:8-161; and 73 Pa. Stat. Ann. § 2303. In Maine, New Hampshire, New York and Rhode Island the safe harbor is in the definition of "personal information" itself; personal information excludes encrypted data (so long as the encryption key has not also been acquired). *See* Me Rev. Stat. tit. 10, § 1347; N.H. Rev. Stat. Ann. § 359-C:19; N.Y. Gen. Bus. L. § 899-aa2; and 11 R.I. Gen. Laws § 11-49.3-3.

[5] Connecticut and New Jersey use the phrase "accessed by." *See* Conn. Gen Stat. § 36a-701b; N.J. Stat. § 56:8-163(a). California, Maine, and New York and Rhode Island use the phrase "acquired by." *See* Cal. Civ. Code §1798.82. Me Rev. Stat. tit. 10, § 1348; N.Y. Gen Bus. L. § 899-aa2; 11 R.I. Gen. Laws § 11-49.3-4. Pennsylvania require both access and acquisition. *See* 73 Pa. Stat. Ann. § 2302 ("accessed *and* acquired") (emphasis added). Massachusetts requires notification in the case of either acquisition or "use." *See* Mass. Gen. Laws § 93H-3(b) ("acquired or used by").

[6] *See* Conn. Gen Stat. § 36a-701b; N.J. Stat. § 56:161 through 56:166 ; N.Y. Gen. Bus. L. § 899-aa2.

[7] *See* 11 R.I. Gen. Laws § 11-49.3-4.

[8] *See* Cal. Civ. Code §§ 1798.150 and 1798.155; Conn. Gen Stat. § 36a-701b(g); Me Rev. Stat. tit. 10, § 1349; Mass. Gen. Laws § 93H-6; N.H. Rev. Stat. Ann. § 359-C:21; N.J. Stat. § 56:8-166(c)(1); N.Y. Gen. Bus. Law § 899-aa.6(a); 73 Pa. Stat. Ann. § 2308; 11 R.I. Gen. Laws § 11-49.3-5. At least one court has found that New Jersey's data breach notification is enforceable by private right of action through the state's consumer protection statute. *See In re Target Corp. Data Sec. Breach Litigation*, 66 F. Supp. 3d 1154, 1167 (D. Minn. 2014).

[9] *See Abdale v. North Shore–Long Island Jewish Health System, Inc., et al.*, --- N.Y.S.3d ----, 2015 WL 4879587, *8 (Sup. Ct. Qns. Cnty. Aug. 14, 2015) (denying health care facilities' motion to dismiss claim for negligence arising from a third-party's theft of sensitive personal information); *In re Target Corp. Data Sec. Breach Litigation*, 66 F. Supp. 3d 1154, 1167 (D. Minn. 2014) (denying retail store's motions to dismiss state claims in purported class action where named plaintiffs alleged that they "actually incurred unauthorized charges to their credit cards; lost access to their accounts; and/or were forced to pay sums such as late fees, card-replacement fees, and credit monitoring costs because the hackers misused their personal financial information.").

[10] *See* Cal. Civ. Code §§ 1798.81, 1798.81.5**;** Conn. Gen Stat. § 42-471; Mass. Regs. Code tit. 201, §§ 17.01-17.05; 11 R.I. Gen. Laws § 11-49.3-2.

[11] Conn. Gen Stat. § 42-471.

[12] 20 U.S.C. § 1232g; 34 CFR Part 99).

[13] Bruce Schneier, Secrets & Lies: Digital Security in a Networked World (John Wiley & Sons, 2000) at page XII.