New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 259—NO. 42

MONDAY, MARCH 5, 2018

Regulatory Gap: **Cybersecurity** at **K-12 Schools**

BY LEORA F. ARDIZZONE AND NICOLE DELLA RAGIONE

© SHUTTERSTOCK

While data breaches at Equifax, Yahoo, Anthem and Target have made the national news, data breaches at school districts are not as widely publicized. Schools are a treasure trove of children's personally identifiable information (PII) (e.g., name, address, Social Security number) and protected health information (PHI), as well as the PII and PHI of faculty and payment card information (e.g., debit and credit card numbers) of parents. Schools are particularly vulnerable to attack because districts with scarce funds must devote them to education, and cannot always divert precious resources to cybersecurity. However, economizing on cybersecurity can be shortsighted. The Federal Trade Commission (FTC) reported that identity thieves often steal children's information from schools, noting that a child's identity is attractive to thieves because it is a "clean slate," enabling a thief to use a child's Social Security number to obtain employment, government benefits, or credit without detection until the child is of age to obtain credit. See Prepared Statement before the Subcommittee on Social Security of the House Committee on Ways and Means on Child Identity Theft Field Hearing Plano, Texas Sept. 1, 2011.

Hackers have victimized a number of school districts. In 2013, Newsday reported that personal data of a number of students in the Sachem School District, in Suffolk County, was posted to an online forum, allegedly by a 17-year-old student in the district. Candice Rudd et al., "Holbrook teen pleads not guilty to hacking charge," Newsday (Nov. 23, 2013). USA Today reported on March 24, 2015, that the Swedesboro-

LEORA F. ARDIZZONE *is of counsel at Ruskin Moscou Faltischek and a member of the cybersecurity and data privacy, regulatory health law and healthcare professionals practice groups.* NICOLE DELLA RAGIONE *is an associate at the firm and a member of its cybersecurity and data privacy practice group.*

Woolwich School District, in New Jersey, was held ransom by hackers. Although the school did not pay the ransom, it lost the use of its systems and had to delay certain web-based testing until its network was rebuilt. Carly Romalino, "Cyberattack disrupts school testing," USA Today (March 24, 2015).

In June 2017, the Miami Herald reported that hackers infiltrated four Florida school district networks in an effort to hack into other government agency systems, including state voter systems. Kyra Gurney, "Hack attacks highlight vulnerability of Florida schools to cyber crooks," Miami Herald (June 18, 2017). The Wall Street Journal reported on Oct. 23, 2017, that in the past year three dozen school systems in the country were hacked resulting in the theft of paychecks and data. Even more distressing, school districts in Montana and Iowa were hacked by actors who accessed student information and sent threatening messages to school officials and parents, including threats to kill children. Tawnell Hobbs, "Hackers Target Nation's Schools," Wall St. J. (Oct. 23, 2017). On Jan. 31, 2018, the FBI issued a Private Industry Notification to the US Department of Education's Office of Inspector General advising of cybercriminal threats directed at schools and students, specifically identifying "The Dark Overlord," which infected systems with ransomware and which may have stolen students' PII. "Private Industry Notification," Fed. Bureau of Investigation, Cyber Div. (Jan. 31, 2018).

While these stories are alarming, the regulatory landscape and enforcement of data breaches affecting schools is not as robust as it is in the health care, banking and retail industries. Schools that receive federal funding are subject to the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g. Generally, FERPA affords parents the right to access their children's educational records, request corrections to those records, and to limit disclosure of a child's educational record. See 20 U.S.C. §1232g; 34 C.F.R. Part 99.

The regulatory landscape and enforcement of **data breaches affecting schools** is not as robust as it is in the health care, banking and retail industries.

While FERPA is designed to protect educational records from disclosure, there is not yet a mandate upon schools to adopt cybersecurity and privacy policies to keep pace with the trends in education to adopt more online teaching tools and curricula, digital record keeping and cybercrime. Moreover, even where a violation of FERPA occurs, there is no private right of action. A parent or student can file a complaint with the U.S. Department of Education (DOE) identifying an alleged violation of FERPA, but enforcement first seeks to obtain voluntary compliance, and only after such efforts fail, the DOE can seek to recover funds improperly spent, withhold payments or sue for enforcement. See 34 CFR §§99.63-67.

The FTC, an emerging player in cyber enforcement, has authority under the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §6501 et. seq. (COPPA). However, COPPA is limited to protecting children under 13, and only applies to commercial websites and online services directed to children under 13, which collect, use or disclose children's PII. A significant component of COPPA is the requirement that commercial sites directed to children under 13 receive verifiable parental consent prior to the collection of a child's PII. An important exception to the rule permits a school to stand in the shoes of a parent where web-based services are offered in schools, solely for the benefit of students and the school and so long as the child's PII will not be used for commercial purposes. "Complying with COPPA: Frequently Asked Questions," U.S. Fed. Trade Comm'n (March 20, 2015). Permitted applications include things like homework help lines, individualized online education modules, online research and web-based testing.

On Dec. 1, 2017, the FTC and DOE hosted a workshop designed to

address trends in education technology including student access to personal computing devices as well as the prevalence of online tools and curricula. Among other things, the workshop sought to clarify how the agencies can ensure student privacy is protected without interfering with education technology. Notably, a panelist, Amelia Vance, from the Education Policy Council at the Future of Privacy Forum, stated, "Schools will never be held liable under COPPA," apparently closing another avenue of mandating security and privacy policies on schools that use commercial applications in education. Transcript: FTC Workshop: Student Privacy and Ed Tech, at p. 15 (Dec. 1, 2017).

Not content to sit on the sidelines of the issue, Gov. Andrew Cuomo signed Education Law §§2-C and 2-D into law on March 31, 2014. These provisions of the Education Law apply, inter alia, to public schools and their third-party contractors. The law charges the Commissioner of the New York State Education Department (NYSED) with promulgating regulations to establish standards for data security and privacy policies to be adopted by New York schools. See N.Y.S. Ed. L. §2-d(5). Although those regulations have not yet been promulgated, the statute requires schools to develop a provisional parents' bill of rights, and third-party contractors, are currently subject to certain provisions of the law if they transmit or receive student data.

Specifically, contracts with third-party contractors must include, inter alia: (1) a data security and privacy plan (Plan) which outlines how state, federal and local data security and privacy requirements will be implemented, (2) have a signed parent bill of rights, (3) prohibition on (a) the use of education records for any purpose other than as expressly provided in the contract, or (b) disclosure of any education records except with appropriate consents or in accordance with applicable law. See N.Y.S. Ed. L. §2(d)(5)(f). Third-party contractors are also required to maintain reasonable administrative, technical and physical safeguards to protect students' PII, and to use encryption technology to protect data while stored or in transit. See N.Y.S. Ed. L. §2(d)(5)(f)(4) and (5). The statute explicitly precludes any private right of action against any school, school district or the NYSED. See N.Y.S. Ed. L., §2-d(7).

It is clear that while there is a duty on the part of schools to protect the privacy of students' educational records (including PII), there is no mandated requirement to adopt and implement specific privacy and security standards as exists in healthcare, banking and retail. Despite the gap in the regulations, schools must be proactive in protecting students' data. The trend towards more online and web-based applications in education, and in electronic record retention is not going to change. Therefore, the risk to children's PII and the integrity of school's networks will only continue to increase. Schools must acknowledge that they are repositories of data desirable to hackers and their portals to educational websites and data storage sites must be secured. School districts should start implementing best practices to meet their duties under FERPA and the NYS Education Law to protect the data of their students. Cybersecurity measures adopted by other industries are instructive, and at minimum, schools should immediately implement the best practices recommended by the FBI to the DOE. See *Private Industry Notification*, supra. Ignoring the lurking danger of a cybersecurity attack until government mandates are enacted is a not only an avoidable mistake, but could well be a breach of a school's federal and state mandates to protect the privacy of their students' identity.