PUBLIC SCHOOL GOVERNANCE AND CYBER SECURITY: SCHOOL DISTRICTS PROVIDE EASY TARGETS FOR CYBER THIEVES

michael a alao

Available at: https://works.bepress.com/michael_alao/1/
Public School Governance and Cyber Security: School Districts Provide Easy Targets for Cyber Thieves

Michael A. Alao, CPA
Salmon P. Chase College of Law
Northern Kentucky University
**Abstract:** School districts rely on information systems to a similar extent as private, business organizations, yet the rules and regulations to ensure that school districts maintain adequate security to prevent data breaches and theft have failed to keep pace with private-sector developments. Advances in the private sector include notice-of-breach laws, consumer protection laws limiting individual liability for fraudulent electronic funds transfers, and auditing and reporting of internal controls. The public sector, including school districts, has also made advances in cyber security rules and regulations, but to a more limited extent than the private sector. Because of the sheer number of public school districts and the laws of fifty states governing public education, this article focuses primarily on Ohio public school districts, although public school districts in other states likely face many if not all the same issues. This article argues that current laws make school districts particularly vulnerable to cyber security threats, but that states can take meaningful steps toward improving cyber security for their school districts without waiting or relying on federal legislation.

**OUTLINE:**

I. INTRODUCTION

II. CURRENT LAW DOES NOT PROVIDE SCHOOL DISTRICTS WITH ADEQUATE CYBER SECURITY
   A. RESPONSIBILITY FOR SCHOOL DISTRICT CYBER SECURITY
   B. DATA BREACH NOTIFICATION LAWS
   C. LIABILITY FOR BANK FRAUD AND THEFT OF PUBLIC FUNDS
   D. GOVERNMENT AND STATE AUDITING STANDARDS

III. ADDRESSING SCHOOL DISTRICT CYBER SECURITY
   A. ADDING GENERAL INFORMATION TECHNOLOGY CONTROLS TO SCHOOL DISTRICT COMPLIANCE REQUIREMENTS
   B. SHIFTING LIABILITY FOR BANK FRAUD TO FINANCIAL INSTITUTIONS

V. CONCLUSION
I. INTRODUCTION

During December 2010 thieves electronically transferred $3.8 million from the Duanesburg Central School District in upstate New York.\(^1\) The school district ultimately recovered $2.55 million, but lost $497,000 in the theft.\(^2\) Crimes involving the unauthorized electronic transfer of funds are not uncommon\(^3\), and cyber criminals often target the most vulnerable organizations, including small businesses, local governments, and public school districts.\(^4\)

This note argues that public school districts have failed to keep up with the private sector with regard to addressing cyber security risks. Public school districts alone are not responsible, however, because, as this article explores, the risks that make public school districts especially vulnerable to cybercrime may require state or state agency action to address those risks. Because of the sheer number of public school districts and the laws of fifty states governing public education, this article focuses primarily on Ohio public school districts, although public school districts in other states likely face many, if not all, of the same issues. Part II of this article begins with descriptions of the laws currently in place that affect overall cyber security for public schools: responsibility for public school cyber security, data breach notification laws, public school district liability for bank fraud losses, and governmental auditing standards. Part II then argues that the current laws in place do not adequately address cyber security for public school districts because (1) responsibility to ensure adequate cyber security lies with each individual

---


2 Id.


school district, (2) exemption from data breach notification laws keeps the public unaware of
cyber-attacks against school district, (3) banking laws subject school district to the same liability
as private businesses for losses resulting from cybercrime, and (4) government auditing
standards focus on the accuracy of school district financial reporting, but not on general
information technology controls. To address the current state of laws, Part III argues for (1) the
inclusion of testing of general information technology controls as part of every school district’s
annual financial audit, and (2) for states to address the lack of protection for school districts in
the Electronic Funds Transfer Act and shift liability from school districts to financial institutions
for losses resulting from cybercrime.

II. CURRENT LAW DOES NOT PROVIDE SCHOOL DISTRICTS WITH ADEQUATE
CYBER SECURITY

No one set of laws or regulations governs cyber security requirements for Ohio public
school districts. Instead, Ohio public school districts must adhere to the requirements of multiple
state and federal regulations ranging from requirements to protect student records\(^5\) to preventing
student access to pornography\(^6\). This part discusses the various laws and regulations applicable

\(^5\) For example, the Family Education Rights and Privacy Act (FERPA) restricts school districts receiving funds from
the Department of Education from disclosing student records. See Andrew B. Serwin, Information Security and
C.F.R. § 99.1(a)(1) to (2)). Risk of unauthorized access to student records exists because Ohio school districts
maintain student records digitally and often provide online access intended for parents, teachers, and other
authorized users. See e.g., http://www.cps-k12.org/academics/monitoring/powerschool/information (describing
student information available to Cincinnati Public School parents through online access to the PowerSchool student
record application).

47 U.S.C. § 254(h)(5), (6) (2000)) (describing the Child Internet Protection Act (CIPA) requirement resulting in
school districts using filtering software to prevent student internet access to pornography).
to Ohio public schools and cyber security, and argues that the laws and regulations currently in place are not adequate to protect school districts from cybercrime.\textsuperscript{7}

A. RESPONSIBILITY FOR SCHOOL DISTRICT CYBER SECURITY

Ohio public school districts must “take reasonable precautions to protect personal information” maintained in school district information systems from “unauthorized modification, destruction, use, or disclosure.”\textsuperscript{8} The statute requires school districts to “appoint one individual to be directly responsible for the system,”\textsuperscript{9} and the school district must develop procedures for using and maintaining the system.\textsuperscript{10} In sum, responsibility for cyber security of information systems lies individually with each of the 611 school districts in Ohio.\textsuperscript{11} This fragmented system of cyber security is inefficient and incomprehensive - most significantly, it leaves school districts to fend for themselves against the complexities of cybercrime.

Financially strapped school districts already face the challenge of maintaining an adequate teaching staff without adding the financial burden of addressing cyber security.\textsuperscript{12} Ohio’s statute does more harm than good for several reasons.

\textsuperscript{8} \texttt{OHIO REV. CODE ANN. \S 1347.05(G) (West 2012); see also Oh. Sch. L. School District Responsibility for Personal Information Systems—System Security and Breach of Security \S 44:10 (2012).}
\textsuperscript{9} \texttt{OHIO REV. CODE ANN. \S 1347.05(A).}
\textsuperscript{10} \texttt{Id. \S 1347.05(F) (“Develop procedures for purposes of monitoring the accuracy, relevance, timeliness, and completeness of the personal information in this system . . . .”)}
\textsuperscript{12} See generally \textit{DeRolph v. State}, 728 N.E.2d 993 (Ohio 2000) (providing and excellent and comprehensive overview of funding problems plaguing Ohio public school districts). The Ohio Supreme Court in \textit{DeRolph} held that the state’s system of funding public education violates the state constitution. \texttt{Id. See also DeRolph v. State, 780 N.E.2d 529, 530 (Ohio 2002) (reiterating the need for a complete overhaul of the state’s public school funding system).}
First, the statute requires that school districts “take reasonable precautions to protect personal information,” but the statute does not provide guidelines with regard to what “reasonable precautions” means.\textsuperscript{13}

Second, the statute requires school districts to appoint one individual “to be directly responsible for the system,”\textsuperscript{14} in effect allowing the school district’s board of education to shift responsibility for cyber security to a single individual. Although not an unusual management structure, having a Chief Technology Officer (“CTO”) or Chief Information Systems Officer (“CIO”) in an Ohio public school district presents its own set of problems.\textsuperscript{15} Under Ohio law, school districts must have an elected board, and the board must then hire and have directly, but separately reporting to it a superintendent and a treasurer.\textsuperscript{16} In essence this creates an organization with a governing board and two chief executives reporting to that board.\textsuperscript{17} Responsibility for academics, general operations, and facilities management lies with the superintendent, while responsibility for the recording, safekeeping, and proper expenditure of school district funds lies with the treasurer.\textsuperscript{18} This division of responsibilities serves its purpose of separating the operation of the school district from the treasury function, but conflicts with the section 1347.05 requirement of appointing one person directly responsible for school district information systems. The conflict arises from the dual reporting organization structure of Ohio

\textsuperscript{13} Compare \textsc{Ohio rev. code ann.} § 1347.05 (requiring school districts to take “reasonable precautions to protect personal information”) \emph{with} \textsc{Ohio admin. code} § 3301-2-11(A) (West 2012) (requiring the Ohio Department of Education to take the same “reasonable precautions,” but providing guidelines to determine the reasonableness of the security precautions). Section 3301-2-11 provides that the Ohio Department of Education (ODE) must, in its determination of reasonable precautions to protect personal information, consider: (1) the nature and vulnerability of the information; (2) physical security of facilities where the information is maintained; and (3) the feasibility of achieving adequate security while balancing cost with the need for the agency and public to access the information. \textit{See} \textsc{Ohio admin. code} § 3301-2-11. Section 3301-2-11(B) goes even further, requiring ODE to “adopt, implement, and enforce a security plan for the protection of personal information.” \textit{Id.}

\textsuperscript{14} \textsc{Ohio rev. code ann.} § 1347.05(A).
school districts. The school board, in accordance with the section 1347.05 requirement could appoint a single CIO responsible for the security of the school district’s information systems, and have that CIO report directly to the board. In practice, however, the CIO, or lower-level equivalent, generally reports to the superintendent, but the superintendent has no authority over the treasurer. Consequently, Ohio school district CIO’s exercise authority over a school district’s information technology infrastructure and information systems, but not the financial system or online banking applications.

Finally, the statute requires Ohio school districts to develop procedures for using and maintaining the system, but again fails to provide guidance as to the minimum requirements and contents for such procedures.

B. DATA BREACH NOTIFICATION LAWS

The Privacy Rights Clearinghouse recorded 695 breaches at educational institutions throughout the United States occurring during the years 2005 through August 31, 2013, potentially disclosing over 11 million records of personal information. These breaches include

---

19 See id. § 1347.05(F)
20 See Privacy Rights Clearinghouse, Chronology of Data Breaches (available at http://www.privacyrights.org/data-breach) (last accessed August 31, 2013). Search criteria included Educational Institutions (EDU); all types of breaches, including unintended disclosure (DISC) (“sensitive information posted publically on a website, mishandled or sent to the wrong party via email, fax, or mail”), hacking or malware (HACK) (“electronic entry by an outside party, malware and spyware”), payment card fraud (CARD) (“fraud involving debit and credit cards that is not accomplished via hacking – e.g., skimming devices at point-of-service terminals”), insider (INSD) (“someone with legitimate access intentionally breaches information – such as an employee or contractor”), physical loss (PHYS) (“lost, discarded or stolen non-electronic records, such as paper documents”), portable device (PORT) (“lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.”), stationary device (STAT) (“lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility”), and unknown (UNKN); and all years 2005 through 2013. See id.
only those made public, and although thirty-four breaches at Ohio colleges and universities occurred, the database reflects only six data breach incidents at Ohio public school districts.\(^\text{24}\)

Ohio Revised Code section 1347 addresses school districts' responsibility for cybersecurity to protect personal information.\(^\text{25}\) Section 1347 defines personal information as a combination of a person’s name and one additional data element such as the person’s social security number, driver’s license number, credit card number, or password to access an individual’s financial account.\(^\text{26}\) School districts, unless exempted, must notify affected Ohio residents of breach of information systems that resulted in authorized access and acquisition of personal information.\(^\text{27}\) The school district must provide notice to residents within forty-five days of discovery of the breach, but only if actual fraud or identity theft occurred or if there exists a “material risk of identity theft or other fraud to the resident.”\(^\text{28}\)

Ohio’s breach notification law applies to state agencies and political subdivisions of the state including school districts.\(^\text{29}\) Other states’ breach notification laws often apply only to businesses and exempt state agencies and school districts.\(^\text{30}\) Four states, Alabama, Kentucky, New Mexico and South Dakota, have no laws requiring either state agencies or businesses to

\(\text{\footnotesize \text{\textsuperscript{24} Id. The inference drawn from the higher number (thirty-four) of data breaches at colleges and universities versus the six breaches during the same period at Ohio public school districts is either (a) colleges and universities are more likely to report breaches, or (b) data breaches occur less frequently at Ohio public school districts. Probably, colleges and universities are more likely than public school districts to report data breaches because colleges and universities tend to be large, have more professional resources, and possess greater awareness of the requirement to give notice of data breaches involving personal information.}}\)

\(\text{\footnotesize \text{\textsuperscript{25} See \textit{Ohio Rev. Code Ann.} \textsection{} 1347.05(G) ("Take reasonable precautions to protect personal information in the system from unauthorized modification, destruction, use or disclosure.") (emphasis added).}}\)

\(\text{\footnotesize \text{\textsuperscript{26} Id. \textsection{} 1347.12.}}\)

\(\text{\footnotesize \text{\textsuperscript{27} Id. \textsection{} 1347.12(B)(1).}}\)

\(\text{\footnotesize \text{\textsuperscript{28} Id.}}\)

\(\text{\footnotesize \text{\textsuperscript{29} Id.}}\)

provide notice of security breaches. But even states with breach notification laws applicable to state agencies and school districts include in their statutes that federal law may preempt the state notification law. Ohio’s breach notification law does not apply to school districts covered under the Health Insurance Portability and Accountability Act of 1996 (‘‘HIPAA’’). Specifically, if the school district provides its employees with health benefits through a self-insured plan, HIPAA privacy rules apply to the plan and preempt Ohio’s breach notification requirements. Breach notification under HIPAA, however, applies only to health information; curiously, it appears to also exempt Ohio school districts from the breach notification requirements for non-health personal information.

Weak and non-existent breach notification laws do not directly affect school district cyber security, but keeping the public in the dark regarding data breaches of school district information systems prevents local communities from putting pressure on school district boards to expend resources to adequately protect those information systems.

---

31 Id. at 1.
32 Id.
33 See Oh. Sch. L. § 44:10 (2012) (citing see R.C. 1347.12(A)(1) (exempting political subdivisions of the state from compliance with Ohio’s breach notification law when the political subdivision is a covered entity under 45 C.F.R. § 160.103); see also Mintz at 36 (“Entities regulated by sections 1171 to 1179 of the ‘Social Security Act,’ chapter 531, 49 Stat. 620 (1935), 42 U.S.C. 1320d to 1320d-8, and any corresponding regulations in 45 C.F.R. Parts 160 and 164 are also exempt [from breach notification].”).
35 See Mintz, supra note 17.
36 See 45 C.F.R. § 164.500(a) (West, Westlaw through 78 Fed. Reg. 46797) (“Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.”).
37 See Oh. Sch. L. § 44:10 n. 2 (2012) (citing see R.C. 1347.12(A)(1), Oh. Sch. L. § 10:20) (“The notification requirements apparently do not apply to a district that is covered by [HIPAA].”). Section 1347.12, Disclosure by State Agency or Agency of Political Subdivision of Breach of Security System; Attorney General Investigation, Civil Action, specifically excludes covered entities as defined in 45 C.F.R. 160.103 from the definition of “agency of a political subdivision.” O HIO REV. CODE ANN. § 1347.12(A)(1). Title 45, section 160.103 of the Code of Federal Regulations defines a “covered entity” as a “health plan, . . . including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise,” and has 50 or more participants or is administered by an entity other than the employer. 45 C.F.R. § 160.103.
C. LIABILITY FOR BANK FRAUD AND THEFT OF PUBLIC FUNDS

Under the Electronic Funds Transfer Act (“EFTA”), school districts that fall victim to cyber thieves through online bank fraud do not receive the same protection as individuals and face having to absorb the losses.\(^{38}\) Regulation E of the EFTA limits the liability of individuals to fifty dollars if individuals give timely notice to financial institutions of financial losses due to online bank fraud.\(^{39}\) Regulation E applies only to individuals, however, and commercial bank account holders such as businesses, not-for-profits, state and local governments, including school districts, typically absorb online bank fraud losses that financial institutions do not recover from the cyber thieves.\(^{40}\)

Commercial bank account holders are not entirely without protection. The Uniform Commercial Code (UCC), under Article 4A, imposes liability for unauthorized transfers on the bank receiving the transfer.\(^{41}\) Article 4A requires the bank receiving the unauthorized transfer to refund the commercial bank account holder any funds transferred plus interest if the commercial bank account holder did not authorize the transfer.\(^{42}\) The receiving bank can, however, escape liability if it proves the following five elements: (1) the bank and account holder agreed to a security procedure verify payment orders, (2) the agreed upon security procedure is a

\[\text{Reference Notes}\]


\(^{39}\) 12 C.F.R. § 205.6(b)(1) (West, Westlaw through 78 Fed. Reg. 46797) (“If the consumer notifies the financial institution within two business days after learning of the loss or theft of the access device, the consumer’s liability shall not exceed the lesser of $50 or the amount of unauthorized transfers that occur before notice to the financial institution.”).

\(^{40}\) See generally Krebs, supra note 38 (Entities that experience similar fraud with a commercial or business banking account do not enjoy the same protections [as holders of individual banking accounts] and often are forced to absorb the losses.”); See also 12 C.F.R. § 205.3 (West, Westlaw through 78 Fed. Reg. 46797) (limiting liability protection under Regulation E of the EFTA to consumer bank accounts).


\(^{42}\) Id. ("[UCC § 4A-204] requires a receiving bank to refund any funds (plus interest) from a payment order that was: (1) not authorized by the customer under UCC § 4A-202; or (2) is not enforceable against the customer under UCC § 4A-203 because the payment order was not caused by (a) an authorized employee or (b) a person who obtained access to the customer’s transmitting facilities, or otherwise obtained transmittal information from the customer.”)
commercially reasonable method to prevent fraudulent transfers, (3) the bank processed the payment order in compliance with the security procedure, (4) the bank accepted the payment order in good faith, and (5) in compliance with any written agreement or instruction of the customer.\textsuperscript{43} If the receiving bank cannot prove all five elements, Article 4A imposes strict liability on the receiving bank for unauthorized electronic fund transfers (EFT).\textsuperscript{44}

Although EFTA and Article 4A of the UCC allocate liability for losses resulting from unauthorized EFT differently based on whether the account holder has an individual or commercial bank account, cyber thieves target individuals and commercial account holders in similar ways.\textsuperscript{45} A common approach is through phishing.\textsuperscript{46} Phishing involves cyber criminals sending spam email\textsuperscript{47} to an unsuspecting customer or bank employee.\textsuperscript{48} The spam email “imitates a message from a legitimate author and is designed to steal personal information through malicious software or lure the recipient into sharing such information.”\textsuperscript{49} For example, cyber thieves hacked into bank customers’ email accounts and then emailed bank employees at the victims’ bank branch the following message:

Good Morning,

Can you please update me with the the available balance in my account and also the information needed to complete an outgoing wire transfer for me today, i am on my way to my nephew funeral service but i will check my mail often for your response.

\textsuperscript{43} Id. (citing UCC 4A-202(b)).
\textsuperscript{44} Id. (citing UCC 4A-204(a)).
\textsuperscript{45}
\textsuperscript{46}
\textsuperscript{48}
Thanks.\textsuperscript{50}

The cyber thieves sent three emails containing the above message to three different branches of the same financial institution.\textsuperscript{51} In two of the three instances, bank employees called the customers and found out that the customer had not sent the email message.\textsuperscript{52} At the third branch, however, the bank employee regularly corresponded with the bank customer via email, and unlike her colleagues at the other branches, responded to the email.\textsuperscript{53} The follow-up email from the cyber thieves instructed the bank teller to transfer money to an account at another bank, which the bank teller did.\textsuperscript{54} In this particular instance the bank accepted fault and agreed to refund the customer the amount fraudulently transferred, and disciplined the employee that processed the transactions.\textsuperscript{55} Under the EFTA the bank would have to refund the individual bank account holder all but fifty dollars of the fraudulently transferred amount.\textsuperscript{56} For a commercial account, however, the bank would only have to refund the customer’s losses only if the bank, as in this example, was at fault or otherwise accepted responsibility.\textsuperscript{57}

The problem for school districts is that they, like businesses and nonprofits, use commercial bank accounts, and as the Duanesburg Central School District example shows, commercial bank account holders do not receive the kind of protection under EFTA afforded to individual bank holders.\textsuperscript{58} Treating local governments, including school districts, like small businesses and non-profits fails to take into consideration that government entities use

\begin{footnotes}
\footnotetext[51]{Id.}
\footnotetext[52]{Id.}
\footnotetext[53]{Id.}
\footnotetext[54]{Id.}
\footnotetext[55]{Id. The bank customer in this example held a commercial account, but cyber thieves target individual and commercial account holders using the same phishing process.
\footnotetext[56]{See Krebs, \textit{supra} notes 38; see also Pinguelo, \textit{supra} note 49.
\footnotetext[57]{See Krebs, \textit{supra} note 1; see also Krebs, \textit{supra} note 38 .
}
\end{footnotes}
commercial banks to deposit public funds.\textsuperscript{59} Essentially, school districts hold public funds in trust, and deposit those public funds with commercial banks for safekeeping. Holding school districts liable for losses resulting from unauthorized EFT ultimately shifts liability to the public. Given that commercial banks benefit and profit from holding public funds, it seems unfair that banks can shift liability for theft of public funds in the banks possession to the public.

D. GOVERNMENT AUDITING STANDARDS

The Comptroller of the United States sets the guidelines for audits of federal government agencies.\textsuperscript{60} Audit practitioners refer to these guidelines as generally accepted government auditing standards (“GAGAS”) or government auditing standards (“GAS”).\textsuperscript{61} State and local governments spending $300,000 or more in federal awards during a fiscal year must comply with the Single Audit Act of 1984, and audits of such state and local governments must adhere to GAS.\textsuperscript{62} Out of Ohio’s 610 school districts, 570 spent federal award money during fiscal year 2012, subjecting them to the Single Audit Act and GAS.\textsuperscript{63}

\textsuperscript{59} See OHIO REV. CODE ANN. § 135.01(K) (“‘Public moneys’ means all moneys in the treasury of the state or any subdivision of the state, or moneys coming lawfully into the possession or custody of the treasurer of state or of the treasurer of any subdivision.”); See also Black's Law Dictionary, FUNDS, (9th ed. 2009) (defining public funds as “the revenue or money of a governmental body,” including “not only coins and paper but also bank deposits and instruments representing investments of public money.”)

\textsuperscript{60} See WARHAM GORHAM & LAMONT, INTERNAL AUDITING MANUAL, 2003 WL 21375208, Government Auditing Standards § B3.01 (RIA 2013).

\textsuperscript{61} Id.


\textsuperscript{63} See OHIO DEP’T OF EDUC., supra note 11. Multiplying column E (average number of district students) by column BB (district federal revenue per student), both in the worksheet titled “District Data,” shows that 570 of Ohio’s 609 school districts received, and likely spent, federal money during fiscal year 2012. Id. Of the 570 school districts receiving federal money, 349 received $1 million or more. Id.
Publicly traded companies, on the other hand, must comply with the requirements of the Sarbanes-Oxley Act. Auditing standards for publicly traded companies significantly changed after passage of the Sarbanes-Oxley Act (“SOX”) in 2002. Most significantly, section 404 of SOX requires corporate management to test and report on the effectiveness of internal controls, and for the external auditors to attest to and report on the management assessment. Part of management’s assessment of internal controls includes testing the effectiveness of information technology general controls (“ITGC”). ITGC include general controls and application controls. General controls apply to all information systems within an organization, including “[information technology (‘IT’)] policies, standards, and guidelines pertaining to IT security and information protection.” Application controls pertain to specific applications and include, among others, automated controls such as requiring the use of individual logons and passwords.

---

65 See generally WARHAM GORMAH & LAMONT, INTERNAL AUDITING MANUAL, 2003 WL 21375206, supra note 60, Generally Accepted Auditing Standards § B2 (noting the need to strengthen investor confidence in the audited financial reports of public companies domiciled in the United States); CCH INCORPORATED, SARBANES-OXLEY MANUAL: A HANDBOOK OF THE ACT AND SEC RULES, 2010 WL 4136243, Foreword (CCH 2008) (noting that “Congress directed the SEC to adopt rules increasing the accountability of senior management, improving the quality of financial reporting, and raising legal and ethical standards for the gatekeepers of the financial system, such as analysts, auditors, audit committees, management, and attorneys.”).
67 See generally WARHAM GORHAM & LAMONT, 2003 WL 21375194, supra note 60, IT General and Application Controls § B1 (providing a comprehensive overview and guidance for management testing of information technology general controls).
68 Id. at § B1.02(3)(b).
69 Id.
70 Id. (“They include controls that help ensure the proper authorization, completeness, accuracy, and validity of transactions, maintenance, and other types of data input. Examples include . . . system-enforced transaction controls that prevent users from performing transactions . . . that are not part of their normal duties.”)
Unlike the requirements under SOX, GAS require only limited evaluation and reporting on internal controls.\textsuperscript{71} External auditors completing school district audits under GAS may review internal controls related specifically to financial statement objectives, but do not provide an audit opinion on the effectiveness of internal controls.\textsuperscript{72} Because school districts do not have to comply with SOX requirements, school districts do not have to test and report on the effectiveness of internal controls, nor do the external auditors provide an opinion on the effectiveness of internal controls. And although audits under both the requirements of SOX and GAS focus on the accuracy of financial statements, an audit under SOX would likely detect and report weak internal controls for online banking transactions where an audit under GAS would not. A SOX audit would reveal an internal control risk such as lax controls over online banking applications because SOX’s requirement that auditors assess the effectiveness of internal controls, including ITGC. A GAS audit, on the other hand, might not reveal such an internal control weakness because lax internal controls for an online banking application do not necessarily affect the accuracy of financial statements.\textsuperscript{73}

\textsuperscript{71} See generally WARHAM GORHAM \& LAMONT, 2003 WL 21375208, supra note 60, Government Auditing Standards § B3.11 (requiring external auditors to address internal controls as part of the audit, but not provide an opinion on the effectiveness of internal controls).

\textsuperscript{72} Id. (“[G]overnment auditors should include in their report . . . . a description of the scope of the auditors' testing of internal control over financial reporting and compliance . . . and the results of those tests or an opinion, if sufficient work was performed . . . .”; See also e.g., OHIO AUDITOR OF STATE, INDEPENDENT AUDITOR’S REPORT OF THE CINCINNATI CITY SCHOOL DISTRICT, HAMILTON COUNTY, FOR THE AUDIT PERIOD JULY 1, 2011 THROUGH JUNE 30, 2012, 3 (Feb. 28, 2013), available at http://www.auditor.state.oh.us/auditsearch/Reports/2013/Cincinnati_CSD_12-Hamilton_resub1.pdf (noting that the auditor completed the audit in accordance with GAS). The external auditor also states, “[W]e have not opined on the effectiveness of the District’s internal control over financial reporting.” Id.

III. UNIFORM CYBER SECURITY STANDARDS FOR SCHOOL DISTRICTS AND
SHIFTING LIABILITY FOR BANK FRAUD FROM SCHOOL DISTRICTS TO
FINANCIAL INSTITUTIONS

This part argues that states should address cyber security for school districts, and
provides two solutions that Ohio specifically should consider implementing.

A. ADDING GENERAL INFORMATION TECHNOLOGY CONTROLS TO SCHOOL
DISTRICT COMPLIANCE REQUIREMENTS

To address the lack of a consistent and comprehensive approach for school districts to
defend themselves from cybercrimes, the Ohio Auditor of State (“OAS”) should develop
minimum required guidelines for school districts, and assess compliance with those guidelines as
part of the financial statement audit of each school district. Ohio already requires the Auditor of
State to complete audits of each school district at least once every two years.74 OAS audits
require auditors to perform tests to determine school district compliance with state laws and
regulations.75 OAS should add compliance with Ohio Revised Code section 1347.05 (requiring
school districts to maintain adequate cyber security) as part of the required compliance tests
auditors must complete as part of a school district financial audit.

74 OHIO REV. CODE ANN. § 117.11(A) (requiring OAS to audit each school districts at least once every two years,
and annually for school districts subject to the Single Audit Act).
75 See id. (“[I]nquiry shall be made . . . whether the laws, rules, ordinances, and orders pertaining to the office have
been observed, and whether the requirements and rules of the auditor of state have been complied with.”); See also
OHIO AUDITOR OF STATE, OHIO COMPLIANCE SUPPLEMENT MANUAL (2013), available at
http://www.auditor.state.oh.us/services/lgs/publications/LocalGovernmentManualsHandbooks/ohio_compliance_su-
plement_manual/2013/OCSJan13.pdf (provides auditors with laws and regulations AOS has identified as
potentially significant in an Ohio local government audit). Conspicuously, the compliance manual does not include
any reference to Ohio Revised Code section 1347.05 and to school districts’ responsibility for cyber security of
information systems. Id.
Modifying the OAS Ohio Compliance Supplement Manual would not require state legislative action\textsuperscript{76}, but state legislators could amend section 1347.05 to require OAS to include testing for compliance with that section as part of the annual or bi-annual audit of school districts. To amend section 1347.05, the Ohio legislature could add a second sub-section stating: “The auditor of state, as part of its audit of school districts in accordance with section 117.11 of the Revised Code, shall report on school district compliance with the requirements of section 1347.05.” Because section 1347.05 requires Ohio school districts to develop procedures for using and maintaining information systems, but fails to provide guidance as to the minimum requirements and contents for such procedures\textsuperscript{77}, the state legislature could further amend section 1347.05 to require OAS to assess and report on the adequacy of such procedures. For example, the legislature could an additional sentence to the proposed second sub-section stating: “In its assessment of the school district’s compliance with the requirements of section 1347.05, and specifically the adequacy of the district’s procedures for using and maintaining information systems, the auditor of state shall take into consideration the balance between the cost of internal controls and the value those internal controls provide.” This particular wording does not provide specific minimum requirements, but instead leaves determination of the adequacy of a school district’s internal controls to the professional judgment of the OAS. The wording does, however, provide an important limitation in its requirement that the cost of the internal control should not exceed the value of the potential harm the internal control seeks to avoid.\textsuperscript{78}

\textsuperscript{76} See OHIO REV. CODE ANN. § 1347.05(F) (“Develop procedures for purposes of monitoring the accuracy, relevance, timeliness, and completeness of the personal information in this system . . . .”).

\textsuperscript{77} See e.g., PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD, Auditing Standards, § 319.23 (“The cost of an entity's internal control should not exceed the benefits that are expected to be derived.”) available at http://pcaobus.org/Standards/Auditing/Pages/AU319.aspx. Although the Public Company Accounting Oversight Board (PCAOB) does not establish government auditing guidelines, the maxim that the cost of an internal control should not exceed the benefit derived from the control applies to all entities, publically held, private, or governmental.
B. SHIFTING LIABILITY FOR BANK FRAUD TO FINANCIAL INSTITUTIONS

Senator Charles Schumer (D–NY) introduced on September 29, 2010 a bill to amend the EFTA to give the same protection afforded to individuals to municipalities and school districts.\(^79\) Specifically, the bill would amend the EFTA to treat municipalities and school districts as “consumers,” and shift liability for losses resulting from cybercrimes to financial institutions.\(^80\) The bill, unfortunately, died in committee.\(^81\)

Given the lack of a national solution to address the lack of protection for school districts in the EFTA,\(^82\) states, state education agencies, or even individual school districts should require commercial banks to assume the liability for losses resulting from online bank fraud. To sidestep the EFTA, school districts can negotiate with financial institutions to assume liability for such losses contractually. Reluctance on behalf of financial institutions to assume such liability exists, of course, but school districts have sufficient bargaining power to overcome such reluctance.\(^83\) Financial institutions that do business with school districts profit from the banking relationship, but school districts and ultimately taxpayers currently foot the bill for losses resulting from online bank fraud. Having commercial banks assume liability for these losses makes for a more

---

\(^79\) See 156 Cong. Rec. S7786-03 (“By Mr. SCHUMER: S. 3898. A bill to amend the Electronic Fund Transfer Act to treat municipalities and school districts as consumers for certain purposes under that Act; to the Committee on Banking, Housing, and Urban Affairs.”); See also Krebs, supra note 38.
\(^80\) See 2009 CONG US S 3898 (the full text of the bill is also available at http://thomas.loc.gov/cgi-bin/query/z?c111:S.3898:).
\(^82\) See generally Krebs, supra note 38 ([E]ntities that experience similar fraud with a commercial or business banking account do not enjoy the same protections [as holders of individual banking accounts] and often are forced to absorb the losses.”); See also 12 C.F.R. § 205.3 (West, Westlaw through 78 Fed. Reg. 46797) (limiting liability protection under Regulation E of the EFTA to consumer bank accounts).
\(^83\) See e.g., OHIO DEP’T OF EDUC., supra note 11. Multiplying column E (average number of district students) by column AW (district total expenditure per student), both in the worksheet titled “District Data,” shows Ohio school districts expended almost $19 billion during fiscal year 2012. Id. The median expenditure per school district during that period was approximately $16 million. Id. Expenditures per school district ranged from $2.7 million, Bettsville Local School District, to $965 million, Columbus City School District. Id.
equitable arrangement, and provides commercial banks with the incentive to help ensure that school districts implement and maintain adequate cyber security measures.

V. CONCLUSION

Public school districts and laws that govern them have failed to keep up with the private sector with regard to addressing cyber security risks. Current laws in place do not adequately address cyber security for public school districts because (1) responsibility to ensure adequate cyber security lies with each individual school district, (2) exemption from data breach notification laws keeps the public unaware of cyber-attacks against school district, (3) banking laws subject school district to the same liability as private businesses for losses resulting from cybercrime, and (4) government auditing standards focus on the accuracy of school district financial reporting, but not on general information technology controls. To address the lack of a consistent and comprehensive approach for school districts to defend themselves from cybercrimes, states should develop minimum required cyber security guidelines for school districts, and assess compliance with those guidelines as part of the financial statement audit of each school district. To address the lack of protection for school districts in the EFTA, states, state education agencies, or even individual school districts should require commercial banks to assume the liability for losses resulting from online bank fraud.