Privacy and the Public Educator

Melissa Dark and Clewin McPherson

Department of Computer and Information Technology, Purdue Univerisity
401 North Grant Street, West Lafayette, IN 47906-2021
{dark, mcpherso}@purdue.edu

Abstract. As of 2003, 99% of K-12 schools in the United States use the Internet. With the increased use of databases and other technologies to manage data in K-12 institutions, an inherent threat to the privacy and confidentiality of that information has also increased. Over the last decade, with the increased use of these technologies, there has also been an increase in the number of privacy-related violations that have occurred, both in industry and in the K-12 environment. There are a plethora of security technologies that can be used to improve privacy; however, organizations such as K-12 schools often cannot afford to hire IT staff versed in the state of the art. Furthermore, technology alone will not address security and privacy problems; policy is an essential ingredient for any organization. This study is a gap analysis investigating privacy practices of public educators in the Midwestern portion of the United States. The significance of the work is that we cannot improve the practices unless we understand deficiencies in current privacy practices and perceptions.

Keywords: Privacy practices, privacy perceptions, privacy risk, public education.

1 Introduction

In 1999, the United States participated in the International Math and Science to determine their ranking in the mathematics and science achievement when compared to the world. The results of the study suggested that new technologies needed to be introduced into the educational system to increase the ranking. As a result, by the end of 1999 the ratio of students to computers in K-12 schools was 6 to 1 [1]. A study conducted in 1995 observed the trends in educational technology and concluded that 1) computers are pervasive in schools, granting almost every child access to a computer, 2) networking is being increasingly used, and 3) educational technology applications have grown significantly and so have their delivery systems [2].

These increasing technologies have not only affected the way teachers deliver their content and students do their research, but also the way in which administrators manage school business. School corporations have become a virtual warehouse of personal information due to the expansive task of managing student, staff and administrative records. As of 2003, 99% of K-12 schools use the Internet [3]; that number has most likely increased since that report.

M.J. Smith, G. Salvendy (Eds.): Human Interface, Part II, HCII 2007, LNCS 4558, pp. 289–298, 2007.

With the increased use of databases and other technologies to manage data in K-12 institutions, an inherent threat to the privacy and confidentiality of that information has also increased. Privacy can be defined in many ways, but can generally be summed up as an individual's ability to control what information is revealed about oneself and who has access to that information [4]. Over the last decade, with the increased use of these technologies, there has also been an increase in the number of privacy related violations that have occurred, both in industry and K-12.

1.1 Privacy Regulations

The increased reliance and utilization of information technology in society has created a need for regulation of the use and abuse of these systems. As technology has increased, the number and scope of the regulations that have been enacted to protect the privacy of information stored and used by these systems has also increased (as illustrated in Figure 1). While not all of the enacted regulations affect K-12 organizations, it is important to understand the general protections that have been placed around information. There are currently over 20 established privacy and privacy-related regulations that affect our daily lives. FERPA, COPPA and HIPAA directly affect the way K-12 organizations are managed. In addition, there are 17 bills that are pending in congress, three of which may affect K-12 institutions [5].

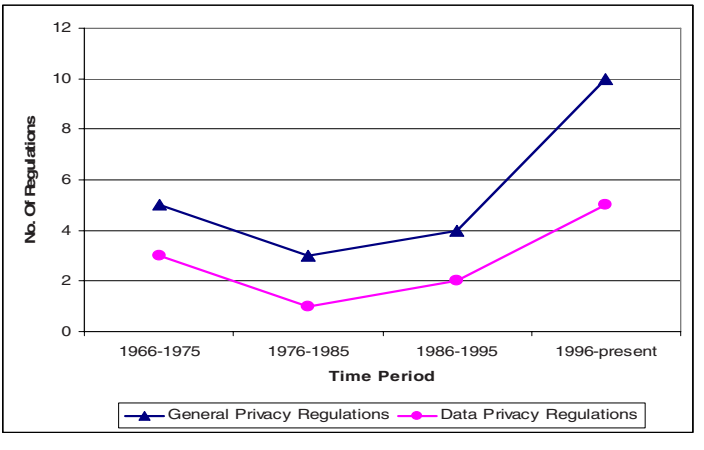

Fig. 1. Privacy related regulations over the last 40 years

Family Educational Rights and Privacy Act of 1974 (FERPA). FERPA was enacted in 1974 and is applicable to all schools that receive funding from the U.S. Department of Education. The regulation protects the privacy of student educational records, which includes any information about a student that is handwritten, in print or stored in electronic format. Educational records include much more than test scores or class standing. They can include health information, description of physical appearance, family economic circumstances, criminal history, ethnic background, political and religious affiliations, and psychological test results. The information can be a fact such as birth date or a Social Security number, and it can include teachers'

opinions of your child [6]. In 1994, several components of FERPA were amended by the Improving America's Schools Act in order to increase the privacy assurances provided for students and families [8].

Children's Online Privacy Protection Act of 1998 (COPPA). Passed in response to the increased online marketing targeting children, COPPA protects the privacy of children (defined as anyone under the age of 13) by requesting consent from a child's parent or legal guardian to collect or use any personal information [9]. While typically the law is focused on commercial websites, it is also applicable to School and District websites that may require the students to provide personal information to access or contribute to the website.

Health Insurance Portability and Accountability Act of 1996 (HIPAA). In 1996 the US Department of Health and Human Services developed a series of rules governing health information. The goal of the rules was to standardize the communication of health information between health care providers and to protect the privacy and security of personally identifiable health information. The information that is protected under HIPAA is any Individually Identifiable Health Information that relates to or includes 1) the individual's past, present or future physical or mental health or condition, 2) the provision of health care to the individual, or 3) the past, present, or future payment for the provision of health care to the individual [10].

It should be noted that the Privacy Rule excludes employment records that a covered entity maintains in its capacity as an employer and education records subject to, or defined in, the FERPA. As a result, while student medical information is covered under FERPA and not HIPAA, any health care information maintained for the purposes of staff and faculty of the school corporation is covered under HIPAA.

Technology is critical to the daily operation of K-12 organizations. These organizations are regulated, much in the same manner as corporations in industry. Unlike these corporations, most K-12 institutions do not have the resources (both financial and technical) to effectively comply with these regulations, while staying abreast of technological advances. It is important to understand exactly where K-12 organizations are in their implementation of privacy protecting principles and technologies in order to design programs and system to enable them not only to be effective in their compliance, but also to take full advantage of the resources and technologies available to them.

2 Current State of K12 Privacy

In March, 2006, an assessment tool, which was designed to assess the state of K12 institutions with regards to various aspects of privacy, was given to a number of technology directors and administrators employed in K-12. The tool was intended to identify the problem space of privacy in the context of each school environment and assess the existence of some suggested privacy preserving strategies and techniques.

2.1 Instrument

The questionnaire was administered online and distributed to 36 schools in the Midwest United States. The survey consisted of 62 questions across five sections – privacy

basics, malware, phishing, responsibility and privacy policies. Each section was assigned a proportionate weight based on the degree of importance to the K12 community in understanding relevant privacy issues. The importance was assigned based on conversations with subject matter experts. Privacy basics, responsibility and privacy policies were weighted equally (25%) as these issues were pivotal to understanding the K12 privacy space. Each question in each of the sections was also assigned a weighting based on how effective the question would be in evaluating the privacy practices of a school corporation and a similar survey provided by Thomas Peltier in his book *Information Security Risk Analysis*, as part of the risk assessment process. For example, in the Privacy basics section, the question "*Is there anyone that is responsible for privacy related issues in the school corporation?*" was weighted higher than "*Are areas containing sensitive information properly secured?*" due to the responsibilities of someone who is responsible for privacy issues in implementing and maintaining privacy preserving strategies and most likely including the securing of sensitive information.

The survey takers were asked to rate each question on a four point Likert scale. The responses were "Yes", "Being Implemented", "Being Discussed" or "No". A "Yes" response would signify total agreement with the question asked. "Being Implemented" means that the corporation is currently implementing systems or processes that would lead to a "Yes" response for that question. "Being Discussed" indicates that the corporation has identified that the practice addressed in the question could be implemented to solve a privacy issue. A "No" response signifies complete disagreement with the stated question. Each response is assigned a numerical weighting, (in a positively worded question, an answer of "Yes" would elicit a score of 4, "Being Implemented" would be scored 3, "Being Discussed would score 2 and "No" would elicit a score of 1). A relative score for the question is then tabulated based on the weighting that was assigned to the question (the takers of the survey did not have any knowledge that the survey was weighted) as shown by Formula 1 below.

$$Q_{1\ \ rel\_weight} = Sum\ (Q_{1\ \ score} * Q_{1\ \ weight}) \tag{1}$$

The relative percentile score for the section is also tabulated as shown by Formula 2.

$$Section\_Score = Sum(Q_{1\ \ rel\_weight} : Q_{7\ \ rel\_weight}) \tag{2}$$

2.2 Population and Sample

The survey was completed by a sample of 26 persons. Ten of those persons were Superintendents, Principals or Assistant Principals, while the other 16 were Technology Directors. The email was sent to the Superintendents and they either completed it themselves or assigned it to the technology director to complete.

3 Results

The results of the survey are reported in the modules according to how the survey was divided. Figure 2 shows that the Privacy Policies section of the assessment yielded

the lowest results from the respondents, while the malware section was significantly higher than the other areas. The maximum score attainable in any section was 100%. Respondents scored over 80% in only one category, and under 50% in two categories.

3.1 Module I – Privacy Basics

The goal of this module was to determine the level of importance and attention that privacy and privacy related issues received in their organizations. Table 1 shows the results of the first module. Overall, the respondents scored just under 60%, which indicates that there is still work to be done in this area of privacy within the various school corporations.

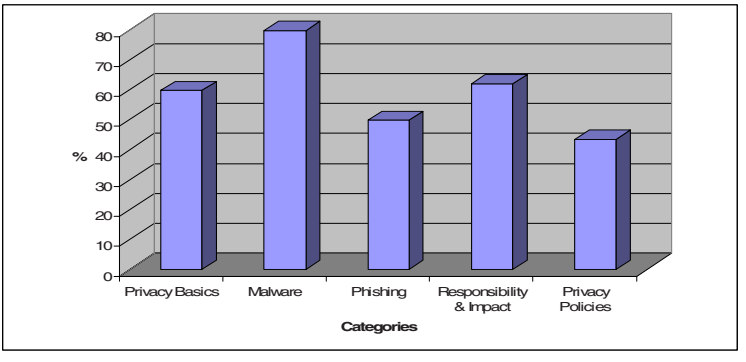

Fig. 2. Survey results by module

Table 1. The privacy basics results

Question	Yes	Being Implemented	Being Discussed	No
1. Does your school corporation separate security and privacy?	26.92%	3.85%	11.54%	57.69%
2. Is there anyone responsible for privacy related issues in the school corporation?	46.15%	0.00%	19.23%	34.62%
3. Is privacy a line item in the budget?	7.69%	0.00%	3.85%	88.46%
4. Is an annual report on privacy compliance issued to management?	0.00%	3.85%	3.85%	92.31%
5. Are areas containing sensitive information properly secured?	61.54%	23.08%	0.00%	15.38%
6. Is confidential information properly secured?	69.23%	15.38%	3.85%	11.54%
7. Are passwords and accounts being shared?	23.08%	3.85%	7.69%	65.38%

Table 1 shows that over 50% of the respondents did not separate privacy and security in their organization and that there is no annual report on compliance with privacy regulations. In most of the schools, there was not a specific person responsible for privacy related issues. This is significant because of the unique privacy specific threats that exist, in addition to fact that privacy preservation in

school corporations is mandated by FERPA. Practically none of the schools had even discussed placing privacy and privacy issues as an item in their budget. It is noted that while a specific focus is not placed directly on privacy, some of the issues are addressed in the organizations, such as the protection of confidential information and the lack of sharing of user accounts and passwords.

3.2 Module II – Malware

The goal of this module was to determine the level of readiness for malware incidents and protection against possible incidents to which these organizations are susceptible. Overall, this module had the highest score of all the modules. Table 2 shows the overall results for this module and indicates that the malware issues were not a significant problem for the school corporations. Most of the institutions had procedures or technology in place to prevent malware from affecting their systems and could identify the sources of malware in their organization.

Table 2. The malware results

	Yes	Sometimes	Rarely	No
1. Do your computer systems block banner ads and "pop ups"?	80.77%	19.23%	0.00%	0.00%
2. Do your computer systems perform at capacity?	53.85%	38.46%	3.85%	3.85%
3. Do you have prevention mechanisms for installation of free and shareware on systems?	53.85%	23.08%	7.69%	15.38%
4. Are administers, teachers and staff prevented from downloading and installing software?	38.46%	34.62%	11.54%	15.38%
5. Is software downloaded from underground warez sites installed on your computer systems?	12.00%	20.00%	24.00%	44.00%
6. Do your browser settings remain constant and unchanged?	65.38%	15.38%	7.69%	11.54%
7. Additional toolbars on your browser are disallowed?	50.00%	26.92%	11.54%	11.54%
8. You organization has mechanisms to ensure that spyware does not negatively affect privacy.	69.23%	23.08%	7.69%	0.00%
9. Viruses have never negatively impacted your corporation.	42.31%	15.38%	30.77%	11.54%
10. Can you identify the major sources of malware in your corporation?	48.00%	28.00%	4.00%	20.00%
11. Are there any technological solutions in place to mitigate malware on your systems?	56.00%	36.00%	0.00%	8.00%
12. Are your employees aware of the dangers of opening attachments in emails?	73.08%	26.92%	0.00%	0.00%

3.3 Module III - Phishing

While the school corporations were generally aware of malware and had sufficient mechanisms in place to preserve the privacy and confidentiality of information from malware, they were not prepared for phishing attacks, as indicated in Table 3.

3.4 Module IV - Responsibility

The responsibility of preserving privacy was the second highest rated area based on the survey (see Table 4). This means that the school corporations recognize the

Table 3. The phishing results

	Yes	Being Implemented	Being Discussed	No
1. Is there any awareness program about phishing attempts?	32.00%	12.00%	12.00%	44.00%
2. Do you think your employees are able to detect phishing attempts?	28.00%	12.00%	12.00%	48.00%
3. Have phishing attacks caused privacy or security problems in the past year?	12.00%	4.00%	8.00%	76.00%
4. Do you block executables?	80.77%	3.85%	3.85%	11.54%
5. Do you block HTML transmitted through email?	29.17%	0.00%	12.50%	58.33%
6. Are you a subscriber to any of the popular phishing scam corporations (ebay, chase, etc)?	15.38%	0.00%	0.00%	84.62%

Table 4. The responsibility results

	Yes	Being Implemented	Being Discussed	No
1. Do you encourage your staff and students to read the privacy statements on websites before registering on it?	73.08%	0.00%	7.69%	19.23%
2. Do you encourage your staff and students to share their personal information only after reviewing privacy statements?	53.85%	3.85%	7.69%	34.62%
3. Are employees trained to be cognizant of privacy matters?	52.00%	16.00%	8.00%	24.00%
4. Is access to sensitive/confidential information by contractors monitored?	73.08%	0.00%	3.85%	23.08%
5. Do employees receive training on privacy relative to their experience and responsibilities?	38.46%	15.38%	7.69%	38.46%
6. Are employees receiving both positive and negative feedback regarding privacy on their performance reviews?	11.54%	0.00%	7.69%	80.77%
7. Are administrators given additional privacy specific training?	7.69%	0.00%	15.38%	76.92%
8. Is there a regular privacy awareness program in place (newsletter, etc)?	0.00%	3.85%	11.54%	84.62%
9. Are audit logs in place for systems containing sensitive information?	38.46%	3.85%	0.00%	57.69%
10. Are violations to privacy tracked?	23.08%	19.23%	11.54%	46.15%
11. Are procedures in place for the proper disposal of confidential information?	48.00%	16.00%	4.00%	32.00%
12. Are unsecured and temporary accounts restricted from sensitive information and disabled in a timely fashion?	80.00%	8.00%	0.00%	12.00%
13. Have employees been trained on proper password management?	56.00%	12.00%	16.00%	16.00%
14. Are permissions being properly set (only those who need the information have access to it)?	92.31%	7.69%	0.00%	0.00%
15. Are users of all network resources required to change the initial default password?	61.54%	7.69%	3.85%	26.92%
16. Are Access Control Lists maintained on a regular basis?	65.38%	11.54%	0.00%	23.08%

importance of privacy in their daily operations and the problem may lie in them not having the resources available to sufficiently deal with privacy risk.

3.5 Module V – Privacy Policies

Privacy policies rated the lowest based on the survey. While all the respondents indicated that they had websites, not all had privacy policies on their websites. In addition, the ones that did have privacy policies had very poorly written policies, in terms of content. In addition, there were no policies or documents that indicated what information was collected by the organization in general or how that information is stored, who has access to it and how it is maintained.

Table 5. The privacy policies results

	Yes	Being Implemented	Being Discussed	No
1. Do you have a website?	100.00%	0.00%	0.00%	0.00%
If the answer to Q1 is yes continue below… If the answer is no, go to Q17				
2. Does your website target group include children under 13?	69.23%	0.00%	0.00%	30.77%
3. Does your website collect email addresses?	19.23%	0.00%	3.85%	76.92%
4. Does your website collect personal identifying information other than email address?	3.85%	0.00%	3.85%	92.31%
5. Is there a privacy policy for your website?	41.67%	12.50%	12.50%	33.33%
If the answer to Q5 is yes continue below… If the answer is no, go to Q16				
6. Does the Privacy Policy mention anything about what specific personal information is collected?	7.69%	0.00%	7.69%	84.62%
7. Does the Privacy Policy mention how the website may use personal information it collects for internal purposes?	11.54%	0.00%	7.69%	80.77%
8. Does the Privacy Policy mention anything about the website's use of personal information collected to send communications to visitors?	12.00%	0.00%	8.00%	80.00%
9. Does the Privacy Policy mention anything about the website's right to disclose personal information to third parties?	8.00%	0.00%	4.00%	88.00%
10. Does the Privacy Policy say whether the website allows users to review, modify and delete some of the personal information collected about them?	4.00%	0.00%	12.00%	84.00%
11. Does the Privacy Policy say what measures the website takes to provide security?	8.00%	0.00%	12.00%	80.00%
12. Does the Privacy Policy say what measures are taken to provide security for personal information during the transmission from the consumer to the website?	4.00%	0.00%	12.00%	84.00%
13. Does the Privacy Policy say what measures are taken to secure personal information after it has been collected?	4.00%	0.00%	12.00%	84.00%
14. Does the Privacy Policy say whether the website places cookies or not?	3.85%	0.00%	11.54%	84.62%

Table 5. (*Continued*)

15. Does the Privacy Policy say whether third parties may place cookies or collect personal information on the website?	3.85%	0.00%	11.54%	84.62%
No privacy policy for the website				
16. Does your corporation have any plans to develop a privacy policy for your website? Answer and then go to Q17	0.00%	12.50%	12.50%	75.00%
No website in the corporation				
17. Do you have a document that describes the type of information collected in your corporation?	26.92%	0.00%	15.38%	57.69%
18. Do you have a policy that documents the privacy practices of your corporation?	34.62%	0.00%	15.38%	50.00%
19. Do information providers have any options when disclosing information?	24.00%	0.00%	16.00%	60.00%
20. Do you have a policy that states the right to disclose personal information to third parties?	30.77%	0.00%	11.54%	57.69%
21. Do you have a policy that states how sensitive information collected is stored and secured?	25.00%	0.00%	12.50%	62.50%

Fewer than half of the respondents (all of whom had a website) had a privacy policy for the website. This is probably not as severe as expected since less than 20% collect email addresses and less than 5% collect personally identifiable information. The section was important, however, since many of the school corporations were considering implementing online student management systems, where parents can access information about their children.

4 Discussion and Implication

One of the most significant things revealed through the results of this study is the discrepancies within responses between the administrators of the school and the technology directors. This indicates that there needs to be a series of conversations between Technology Administrators and Superintendents, where the topic is privacy and privacy related issues. An important precursor to this conversation is the other main observation that can be drawn from this study – the need for privacy education for all those involved in the administration and operation of school corporations. This is significant since 3 of the five areas yielded very poor results (under 60%). The conversation between these education leaders cannot be effective unless and until both parties can use the same vocabulary, understand the important of privacy in their organizations, understand their role in privacy preservation and identify the threats and vulnerabilities that their organizations face.

5 Conclusion

Privacy is important to K12 organizations. Not only is it important because of civil responsibility, but it is also important because it is mandated by law. K12 organizations are currently unprepared to deal with the threats to privacy and in most

cases, do not understand their role in protecting the privacy of their constituents. It is important that K12 personnel be educated about privacy within the constructs of their organizations and that management have a common vocabulary and understanding of these issues.

Acknowledgments. This material is based upon work supported by the National Science Foundation under Grant No. 0430274. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

1. Smerdon, B., Cronen, S., Lanahan, L., Anderson, J., Iannotti, N., Angeles, J.: Teachers' tools for the 21st century: A report on teachers' use of technology (NCES Publication No. 2000-102). Washington: U.S. Department of Education, Office of Educational Research and Improvement, National Center for Education Statistics. Retrieved October 15, 2006 (2000) from http://nces.ed.gov/pubs2000/2000102A.pdf
2. Ely, D., Plotnik, E.: Trends in Educational Technology 1995. ERIC Digest, ERIC Clearinghouse on Information and Technology, Syracuse New York (1996) ED398861
3. U.S Department of Education, National Center for Educational Statistics. Internet Access in Public Schools and Classrooms: 1994 – 2002, NCES 2004-011. Washington, D.C (2003)
4. Brandeis, L., Warren, S.: The Right to Privacy. Harvard Law. Review 4, 193 (1890)
5. EPIC, EPIC Bill Track: Tracking Privacy, Speech, and Cyber-Liberties Bills in the 109th Congress. Electronic Privacy Information Center (EPIC). Retrieved October 22, 2006 (2005) from http://www.epic.org/privacy/bill_track.html
6. Privacy Rights Clearinghouse, Privacy in Education: A Guide for Parents and Adult-Age Students. Privacy Rights Clearinghouse. Retrieved October 22, 2006 (2006) from http://www.privacyrights.org/fs/fs29-education.htm#3
7. U.S Department of Education. Family Educational Rights and Privacy Act (FERPA). Ed.gov. Retrieved on 16th October 2006 (2005) from http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
8. U.S Department of Education. Legislative History of Major FERPA Provisions. Ed.gov. Retrieved on 16th October, 2006 (2004) from http://www.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html
9. Federal Trade Commission. Children's Online Privacy Protection Act of 1998. Retrieved on 17th October, 2006 (1998) from http://www.ftc.gov/ogc/coppa1.htm
10. Privacy Rights Clearinghouse. HIPAA Basics: Medical Privacy in the Electronic Age. Privacy Rights Clearinghouse. Retrieved October 22, 2006 (2006) from http://www.privacyrights.org/fs/fs8a-hipaa.htm