CERIAS Tech Report 2004-28

KEEPING INFORMATION SAFE: AN EXPLORATION OF TEACHER PRACTICE AND PERCEPTIONS IN K-12 SCHOOLS

by Matt Rose and Dazhi Yang

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

KEEPING INFORMATION SAFE: AN EXPLORATION OF TEACHER PRACTICE AND PERCEPTIONS IN K-12 SCHOOL

Matt Rose, Center for Education and Research in Information Assurance and Security, Purdue University, USA mrose@cerias.purdue.edu
Dazhi Yang, Educational Technology, Purdue University, USA dyang@purdue.edu

ABSTRACT

As schools become more dependent on information technology to facilitate administrative tasks and enhance learning and discovery, the security of the schools' information systems, the data that resides on those systems, and even the safety and privacy of the systems' users is becoming a growing concern. Federal regulations, due diligence, and student safety are only a few of the motivating factors that serve to illustrate the importance of information security. Unfortunately, little has been done to record the current state of information security in K-12 educational institutions, including the current state of teacher practice and perception.

This report summarizes a study of the practice and perceptions of information security in participating Indiana K-12 schools. In particular, the study investigated teacher perceptions and practices related to information protection and assurance for K-12 educators and support staff. Two comprehensive online surveys, a technology coordinator survey and a teacher survey, were conducted to collect data about current practices and perceptions regarding information security in K-12 schools in the state of Indiana. Quantitative data were collected and analyzed in the following areas: general information security needs; file management/backup and software issues, email and password security issues, physical threats and social engineering issues, copyright and fair use, compliance with FERPA regulations, and Internet threats. In addition, data about the perceived importance of the topics and which topic(s) the K-12 audiences need to learn about were recorded and prioritized.

INTRODUCTION

Information security incidents are pervasive; according to the 2003 CSI/FBI Computer Crime and Security Survey, 56% of the respondents detected unauthorized use within one year's time (Computer Security Institute, 2003). Information security incidents affect society on the individual, organizational, national, and global levels. Security incidents adversely affect individuals, who lose valuable, sensitive information and services; these incidents affect organizations, who spend valuable resources preventing, detecting, and responding to incidents, and who suffer lost revenue and opportunity. Information security incidents also have the potential to affect the nation's security, whose critical infrastructure depends on telecommunications and the Internet for core business and functional services. Therefore, "the security of cyberspace rests on the security of all its components" (President's Critical Infrastructure Protection Board, 2002).

Information security is a growing concern for K-12 schools, since most schools now use information technology for organizing and accessing data as well as to facilitate learning. In fact, K-12 schools have embraced information technology as an effective tool for engaging students in the learning process and streamlining teacher productivity. With increased federal legislation and funding in support of increased access to educational technology, American schools have seen an explosive growth of information technology in the classroom. The Telecommunications Act of 1996 expanded Internet access to K-12 schools; as a result 99% of K-12 schools use the Internet. (U.S. Department of Education, 2003).

With increased access comes increased responsibility. For example, personally identifiable information of students and staff is made much more easily available. However, academic records must be secured, and sensitive information must be restricted in its availability. Federal privacy regulations such as the Family Educational Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA), as well as school improvement initiatives such as No Child Left Behind, all serve to highlight the importance of protecting sensitive information.

The Center for Education and Research in Information Security (CERIAS) and Infotex, conducted a pilot study of vulnerabilities in K-12 systems in the state of Indiana. This study showed that the IT systems of K-12 schools are vulnerable; as an example, 40% of the participating schools were easily penetrated from the Internet, 100% of the schools' CIPA protection measures were easily circumvented using basic tools and techniques well within the grasp of an average student, and payroll and grade systems were relatively easily penetrated in 90% of the participants (CERIAS K-12 Outreach Program, 2002, p3). These vulnerabilities have potential downstream implications for misuse of data, misuse of system services, personal safety, crimes against children, public embarrassment to schools and so on. For example, confidential and sensitive information can be stolen, lost, and exposed to the public. The threats and vulnerabilities associated with school information systems are especially pertinent to K-12 educators and support staff, who are obligated to protect sensitive information such as assessment data under the Family Educational Rights and Privacy Act, or FERPA, one of the nation's strongest privacy protection laws.

A prevalent misconception concerning information security is that threats and vulnerabilities are generally best-addressed with technical solutions. Many factors affect information security in an organization, and not all of them concern the technical aspects of computers and networks. In fact, the practice of information security transcends many aspects of computers and networks and is actually one of the most critical policy and structure decisions in any organization, including school systems. "People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems (Schneier, 2000, p. 255). Therefore, administrators, technology staff, and teachers have the same responsibility to ensure the security of a school's information systems, including data, equipment, and services, and even the users of these systems.

Although the information security of K-12 school systems is—or perhaps should be—an utmost priority, the current state of information security awareness in K-12 educational institutions is largely unknown and unrepresented. To date, very little has been done to collect and analyze the practices and perceptions of K-12 audiences in terms of information protection and assurance.

BACKGROUND

The CERIAS K-12 Outreach Program conducted a preliminary exploratory study concerning the current level of teacher awareness in terms of keeping information safe in K-12 schools. The goal of this study was to assess the specific needs of the K-12 audiences in regard to information protection and assurance. The primary participants of this study were K-12 educators who hold a bachelor's and /or master's degree in education or a related field. Specifically, the primary purposes of this study were:

- to collect data concerning practices and perceptions of information protection and assurance from teachers and technology coordinators in K-12 schools in the state of Indiana;
- to identify the gap of current level of practices and perceptions in terms of information security and the compliance of computer use with FERPA and the desired level of practice and perceptions;
- to determine the specific needs of information security and the compliance of computer use with FERPA regulations for K-12 audiences.

METHODOLOGY

Two quantitative online surveys were used to collect data. The first survey was administered to Indiana K-12 technology coordinators, and the second was administered to in-service K-12 teachers in the state of Indiana. Several methods of advertisement were used to announce the surveys and solicit participation. The surveys were announced on the CERIAS K-12 outreach program website, and the Wabash Valley Education Center (WVEC) sent solicitation emails to its member school corporations. (The WVEC is one of nine educational service centers in the state of Indiana; its purpose is to serve as a cooperative service to participating schools. The Center serves 35 public school corporations, 5 non-public schools and one area vocational school involving over 70,000 students in 154 school buildings. The membership also includes over 5,000 teachers and administrators.) Voluntary participants submitted the survey online during a six month period.

Technology coordinators were asked to identify the practices and perceptions of information security both for themselves and their teachers. Teachers were asked to identify their own practices and perceptions of information security as well as their knowledge of specific information security issues. This approach maintains that data from multiple sources and different perspectives could serve the purpose of triangulation. In triangulation, multiple sources "enhance the understanding of a phenomenon and research problem" (Rossman & Wilson, 1985, cited in Cresweel, 2002, p562). In the context of this assessment, a triangulated approach was used to combine data from technology coordinators and teachers. Survey data was compiled and frequencies are reported in the results section of this paper.

RESULTS

Technology Coordinator Demographic Information

There were 43 responses to the Technology Coordinator Survey. At least 80% of the participating technology coordinators were from rural public schools with a population of at least 50 teachers and an infrastructure of more than 200 computers. Approximately 84% of the technology coordinators reported that their schools had at least four file servers and also maintained a web server. The respondents varied in years of working experiences; more than half had one to fifteen years of experience; nearly 44% had more than fifteen years of experience.

Approximately 51% of the technology coordinators reported that their current job responsibilities included aspects of system administration, network administration, desktop/technical support for faculty & staff, and school web site design and maintenance. Nearly 70% of the technology coordinators were in charge of information security management, professional development, and administration or management of their school's technology facilities and network. Nineteen percent of the technology coordinators were also full-time teachers.

Information Security Policies and Procedures in K-12 Schools

Approximately 80% of the respondents indicated that information security was "very" or "fairly important" for their teachers and schools. However, only approximately 70% of the respondents indicated that their school had written information security policies. Generally speaking, information security policies included policies, rules, standards, and procedures which were related to information security and assurance in the context of schools. Of these respondents, approximately 73% reported that their information policies were easily available.

Table 1: Information Security Policies

Question: Does your school have information security policies?		
Answer	Yes	No
Percent	70%	30%
Question: If applicable, are information security policies easily available?		
Answer	Yes	No
Percent	73%	27%

Seventy-nine percent of the technology coordinators indicated that their school had formal information incident reporting procedures, whereas 21% of the technology coordinators indicated that their school had no such procedures. However, having formal information incident reporting procedures did not mean that all the teachers and/or staff members could report the incidents properly. According to the survey, less than 10% of the technology coordinators indicated that their teachers and/or other staff members knew how to properly report information incidents according to the reporting procedures. In addition, only 35% of the technology coordinators reported that their teachers knew the consequences of failing to comply with information security policies.

Perceptions of Teacher Knowledge & Practice: Operating System & Virus Issues

When asked which operating systems security issue(s) the teachers were familiar with by choosing from disk corruption, file corruption, and system vulnerabilities and holes, approximately 49% of the technology coordinators chose "disk corruption and file corruption"; nearly 16% chose "system vulnerabilities and holes", and nearly 45% indicated that they were not sure.

As for how to use antivirus programs, approximately 60% of the technology coordinators indicated that their teachers or most of their teachers knew how to use at least one antivirus program. However, nearly 37% indicated that their teachers did not know how to use any antivirus program at all. At the same time, only approximately 35% of the technology coordinators reported that their teachers or most of their teachers knew how to avoid viruses in general.

Email & Password Issues

Approximately 69% of the technology coordinators indicated that their teachers or most of their teachers knew there were overall risks to use of email. Specifically, a large majority (91%) of the technology coordinators reported that their teachers were aware that viruses and other malicious codes could infect their computer systems through email attachments.

Table 2: Risks to Email Security

Question: Do your teachers know there are risks to email communication?				
Response	Yes	Most Do	Most Don't	No
Percent	39%	30%	29%	2%
Question: Do your teachers know that viruses and other malicious codes could get into the computer system through email attachments?				
Response	Yes		No	
Percent	91%		9%	

Regarding secure password practices, approximately 56% of the technology coordinators responded that most of their teachers knew how to choose a safe login password. However, only 14% of the technology coordinators reported that their teachers changed their passwords very often; the majority (84%) of the respondents noted that their teachers seldom or never changed their passwords, while the remaining 2% were "not sure". Further, approximately 35% of the technology coordinators reported that their teachers either often wrote their passwords on Post-It Note or left their computers without enabling password protection.

Physical Security & Social Engineering Issues

From the Technology Coordinator Survey, approximately 86% of the technology coordinators responded that their teachers perceived the technology coordinator as responsible for the physical security of the school information systems; and nearly 30% of the responses indicated that their teachers perceived that the school administration was responsible for the physical aspect of the school information systems security.

A large majority (91%) of the technology coordinators reported that their teachers left floppy disks, CD-ROMs, and other storage media on desks and/or in unlocked drawers. Approximately 63% of the technology coordinators reported that their teachers placed or allowed food/drink

near computer equipment. In addition, 91% of the technology coordinators reported that their teachers would leave classroom doors unlocked, and computer equipment unattended.

Approximately 56% of the technology coordinators indicated that their teachers or most of their teachers were not cognizant of social engineering ploys, such as dumpster diving and shoulder surfing. Only a very small percent (5%) of the responses indicated that their teachers or most of their teachers were aware of such social engineering issues. In addition, 9% of the technology coordinators reported that their teachers had been the victims of such ploys; 79% answered that they were not sure; and the rest of 12% indicated that their teachers had never been the victims of any social engineering ploy.

Table 3: Physical Security Issues

Issues	Unsecured storage media	Unsecured practices with computer equipment	Unsecured computers, and technology equipment and facilities
Percent	91%	63%	91%

Copyright and Internet Issues

All the participating technology coordinators reported that their schools used filtering software. However, when asked whether their teachers were aware of online threats to the students, such as potential abductions, sex predators, and so on, approximately 63% indicated that their teachers or most of their teachers were aware of online threats, 14% indicated that their teachers or most of their teachers were not aware of such threats, and the others (23%) either indicated "not sure" or "some were aware and some were not" (see Table 4).

Table 4: Technology Coordinator's Perception of Teachers' Awareness of Online Threats to Students

Question: Are your teachers aware of online threats to their students?						
Response	Yes	No	Most Are	Most Aren't	Some Are, Some Aren't	Not Sure
Percent	23%	5%	40%	9%	18%	5%

The wide spread use of computers and the Internet makes copying and duplicating copyrighted materials much easier than ever for both students and teachers. Although approximately 72% of the technology coordinators reported that their teachers knew about copyright violation, more than half of the technology coordinators reported that their teachers had violated copyright law (see Table 5). Further, nearly 37% of the technology coordinators reported that their teachers or most of their teachers knew about fair use, but more than half of the responses indicated that their teachers or most of their teachers had abused fair use (see Table 6).

Table 5: Teachers' Violation of Copyright

Question: Have your teachers ever violated copyright law?			
Response	Yes	No	Not Sure
Percent	53%	0%	47%

Table 6: Teachers' Abuse of Fair Use

Question: Have your teachers abused fair use?			
Response	Yes	No	Not Sure
Percent	51%	0%	49%

FERPA Compliance

Approximately 59% of the technology coordinators reported that their teachers did not understand how FERPA regulations applied to the computer use in K-12 schools (see Table 7). Further, nearly half of the technology coordinators responded that their teachers did not know the definition of personally indefinable information according to FERPA. Therefore, it was not surprising that more than half of the technology coordinators reported that their teachers or most of their teachers did not know the possible consequences of failing to comply with FERPA.

Table 7: FERPA Regulations and Computer Use

Question: Do your teachers understand how FERPA regulations apply to the computer use in K-12 schools?							
Response	Yes	No	Most Do	Most Don't	Some Do, Some Don't	Not Sure	Not Applicable
Percent	0%	27%	5%	32%	7%	27%	2%

Professional Development Needs

The technology coordinators identified several potential information security awareness and education topics for their teachers' professional development (see Table 8). "Compliance of computer use with FERPA" was identified as the number one instructional need, although technology coordinators were allowed to select multiple topics. The following table summarizes the technology coordinators' choices for the future information security professional development opportunities for K-12 educators.

Table 8: Professional Development Needs

Question: Which topic(s) do you think your teachers need to learn about?	
Topic	Percent
Compliance of computer use with FERPA	88%
Copyright violation and fair use	28%
File management & backup	28%
Email practice and security	26%
Passwords practice and security	26%
Software and Internet issues	26%
Physical threats to hardware, storage media and printed material	23%
Social engineering attacks	23%
Steps to eliminate threats to physical threats	19%
All the above topics	*12%*

Teacher Demographic Information

There were 68 responses to the Teacher Survey. At least 76% of the participating teachers were from rural public schools. Almost all of the participating teachers had at least one computer in their classroom and approximately 60% of the participating teachers had twenty to thirty students

per class. Approximately 28% were elementary teachers, 26% middle schools teachers, and 46% high school teachers. The participating teachers covered nearly all subject areas. They varied in years of teaching experiences; nearly 40% of them had one to eight years of experience; and nearly 46% had even more than twenty-five years of teaching experience.

Perceptions of Knowledge & Practice of Information Security

Approximately 90% of the teachers responded that information security was very or fairly important for their schools. However, only half of the teachers reported that they had some sort of training in information security in the last twelve months, and nearly 30% of the teachers reported that they have never had any information security training.

File Management, Software Issues and Virus Issues

Approximately 27% of the teachers reported that they backed up files every day, nearly 16% backed up files once a week, and 19% of the teachers reported that they never backed up their files. Although more than half of the teachers (58%) considered system vulnerabilities and holes the primary security issues for operating systems, 15% of the teachers considered disk and file corruption the primary security issues, and 27% of the teachers were not sure what security issues there were with operating systems.

Approximately 68% of the teachers responded that they never used peer-to-peer programs, such as Kazaa or Napster, 29% used peer-to-peer programs once in a while, and nearly 3% of the teachers used such a program every day. In addition, approximately 46% of the teachers reported that their students never used any peer-to-peer programs at schools; 17% reported their students used such program sometimes, and the other 37% did not know whether their students used these applications.

Approximately 68% of the teachers could identify a specific antivirus program on their school computers; 31% of the teachers could not; and only 1% of the teachers indicated that they were not aware of an antivirus program on their school computers.

Approximately 36% of the teachers would check for details if an automatic update window appeared, whereas 21% would choose “remind me later” and nearly 43% of the teachers would ignore or close the pop up window.

Email & Password Issues

Most of the teachers (approximately 85%) knew that minimizing the use of attachments was a safe email practice. And 88% of the teachers would check with reputable sources to see if it was a hoax when they received an email warning about a new virus. Approximately 73% of the teachers could identify the most prevalent ways which viruses and other malicious codes could get into the computer system, such as minimizing the use of attachments or not opening an email attachment.

Approximately 80% of the teachers could successfully choose a safer password when given four different example passwords, although they were not asked to justify their response. Additionally, approximately 30% of the teachers changed their passwords very often (once every

90 days), approximately 39% of the teachers seldom changed their passwords, and another 31% never changed their passwords.

Physical Security & Social Engineering Issues

Approximately 78% of the teachers agreed that everyone within the school should be responsible for the physical security of information systems; however more than one third of the teachers were not aware of that writing passwords on Post-It Notes, leaving computers on without protection, and using weak passwords could cause an information security incident.

Further, only 43% of the teachers could identify three major physical threats to technology equipment and facilities. Last but not least, only nearly 44% of the teachers could successfully identify poor physical security practice examples.

Table 10: Physical Security Threats

Question: Which is (are) the physical threat(s) for computer technology equipment and facilities?					
Threat	Intentional Threats (Damages)	Accidental Threats (Damages)	Environmental Threats (Damages)	All of the Above	Not Sure
Percent	64%	57%	53%	43%	16%

Table 11: Poor Physical Security Practices

Question: Which of the following is (are) poor physical security practice example(s)?					
Example	Leaving file storage (floppy disks, CD-ROMs, and etc.) on desks or in unlocked drawers	Allowing food/drink near computer equipment	Leaving classroom doors unlocked & computer equipment on when away	All of the Above	Not Sure
Percent	69%	76%	87%	44%	0%

As to what precautions should be adopted to control or eliminate physical security threats in K-12 schools, only 49% of the teachers were able to adopt a more comprehensive approach towards the physical security of computer information assets.

Table 12: Precautions Towards Physical Security of Computer Information Assets

Question: Which is (are) a precaution (s) that you should practice to ensure the physical security of your computer information assets?					
Precaution	Do not grant unauthorized access to equipment	Use timed password locks on computer monitor	Control the environment where the computers are placed	All of the Above	Not Sure
Percent	71%	56%	79%	49%	3%

The Teacher Survey data showed that the majority teachers had little knowledge about social engineering issues. Approximately 65% of the teachers were not sure what social engineering ploys were even given some very common social engineering incidents, such as dumpster diving,

voice disguising and so on. This result was congruent with the Technology Coordinator Survey, since approximately 56% of the technology coordinators indicated that their teachers or most of their teachers were not aware of social engineering ploys.

Copyright and Internet Issues

The teachers' level of knowledge about specific copyright issues varied. For example, approximately 61% of the teachers knew that installing one copy of copyrighted software to all the classroom workstations violated copyright law; however, nearly 26% of the teachers considered it legal to allow students to access copyright-protected software on a central server from all classroom workstations without considering the implications.

The survey data showed that the teachers did not completely understand fair use, and some of them abused it. For example, nearly 41% considered it fair use to sell copies of a multimedia CD-ROM (such as a science fair multimedia CD-ROM) to recover the costs of reproduction. In this case, the teachers ignored the fact that fair use only allows educational use of copyrighted material, but that there is no anticipation of wider distribution, even if everything in the CD-ROM was copied under fair use guidelines. Further, nearly 20% of the participating teachers skipped the fair use question on the survey, which might have demonstrated that some of the teachers were not familiar with fair use.

Approximately 89% of the teachers reported that their schools used filtering software for Internet access. However, 2% of the teachers reported that their school did not use any filtering software, and another 2% of the teachers reported that teachers in their school were supposed to supervise student use of the Internet. The other 7% of the teachers responded that they did not know whether their school used filtering software or not.

Data from the Teacher Survey showed that most of the teachers were aware of possible online threats to their students. These online threats identified by the teachers in this survey might have been the teachers' concerns with their students' use of Internet as well.

Table 13: Possible Online Threats to Students

Question: What are the online threats to students?					
Online Threats	Exposure to pornography	Release of personal information	Kidnapping or Abduction	Harassment	Not sure
Percent	92%	91%	69%	0%	2%

FERPA Compliance

Approximately 73% of the teachers could successfully identify personally identifiable information according to FERPA when given the choices of student's name, family address, social security number, test identifying number, and so on; however, there were still nearly 14% of the teachers who could not completely identify personally identifiable information. Unfortunately, approximately 29% of the participating teachers skipped the question. This might indicate that some of the teachers did not completely understand FERPA, or the consequences of failing to comply with FERPA. In fact, there was no teacher who could identify all the correct statements for this question when given some possible consequences (see Table 14).

Table 14: Possible Consequences of Failing to Comply with FERPA

Question: What are the possible consequences of failing to comply with FERPA?				
Statement	Law suits /fines	Damages to the school's reputation	Termination of eligibility to receive government funding	All of the Above
Percent	96%	71%	71%	0%

Professional Development Needs

The teachers identified several potential information security awareness and education topics of interest for their own professional development (see Table 15). Unlike the technology coordinator survey, which found that FERPA compliance was the number one instructional need, copyright violation and fair use was the number one topic. In addition, nearly 34% of the teachers indicated that they wanted/needed to learn all the topics mentioned in the survey.

Table 15: Professional Development Needs

Topic	Percent
Copyright violation and fair use	33%
Software and Internet issues	27%
Compliance with FERPA	25%
Social engineering attacks	19%
File management & back	19%
Email practice and security	16%
Steps to eliminate threats to physical security	14%
Physical threats to hardware, storage media and printed material	10%
Passwords practice and security	6%
I want to learn more about all the above topics.	35%

CONCLUSION AND RECOMMENDATIONS

The results of this study illustrate the current state of information security awareness and practice in the participating schools. Both the majority of the technology coordinators (80%) and the teachers (90%) indicated that information security was "very" or "fairly important" in their schools. However, nearly one third of the schools didn't have written information policies, procedures and standards, according to the technology coordinators. This is alarming, considering that 99% of K-12 schools receive E-rate funding and are thus obligated by CIPA to maintain at least an acceptable use policy (U.S. Department of Education, 2003). Even if the schools did have written information security policies, not all of them made such polices easily available. Similarly, although some schools had incident reporting procedures, not all of the teachers could follow them appropriately. Furthermore, nearly 30% of the teachers reported that they had never received training in information security, and only half of teachers reported that they had some training in the last twelve months. Information security awareness and training activities are generally considered a best-practice in information technology management. All users of an organization's information system "should receive appropriate training and regular updates in organizational policies and procedures. This includes security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities" (ISO 2000, p. 11). Based upon the results of the study, the majority of the participating schools need to better create, maintain, and disseminate their information security policies and procedures.

As an example, both surveys showed that at least half of the teachers didn't have adequate knowledge about operating system security, nor did half of the teachers know how to avoid viruses in general. The teacher survey data indicated that only one third of the teachers would update their operating systems when prompted. Surprisingly, the teacher survey data also showed that 3% of the teachers used some sort of peer-to-peer program to download material every day, suggesting that copyright violation may extend beyond the "beg, borrow, and steal" mentality prevalent in K-12 schools. Peer-to-peer programs facilitate illegal file sharing and are the primary vehicle for music and software piracy; in addition, peer-to-peer programs are highly insecure and are known to introduce a host of new vulnerabilities to a user's operating system. The perceived importance of operating system security is relatively low, as indicated by the low number of teachers interested in learning about software and Internet issues. This suggests that professional development opportunities that emphasize both the procedures for securing operating systems as well as the underlying reasons for practicing operating system security are needed.

In regards to email security and the risks associated with use of email attachments, the majority of educators, 85%, were aware of these issues; in fact, in this case, teacher awareness was higher than anticipated by technology coordinators. Unfortunately, teachers were not as aware of password security practices. While teachers generally could choose a safe password, they seldom change or protect their own passwords. Thirty-five percent of the technology coordinator respondents noted that their teachers wrote down their passwords or left their computer accounts unattended, which is congruent with results from the teacher survey that indicated that approximately one third of the teachers were not aware that writing passwords on Post-It-Notes and leaving computer accounts on without protection could cause an information security incident. Possible professional development opportunities in this area include the creation and dissemination of password security guidelines, as well as background training on the purpose and function of passwords and associated account access issues.

Related to account access is physical security. There were significant gaps between what teachers reported and practiced regarding physical security issues. While eighty-seven percent of the teachers surveyed felt that leaving classroom doors unlocked and computer equipment on when away was an insecure practice, ninety-one percent of the technology coordinators reported that their teachers did in fact leave classrooms and computers unattended. This gap between the teacher reports and their actual practice could be attributed to a number of factors: Teachers may not completely understand the ramifications of unauthorized use of their accounts by a third party, there may be a lack of communication on the part of the school system, there may be a lack of organizational policy regarding account access and physical security, or it could be a combination of several factors.

Teachers were generally more aware of social engineering ploys than thought by the technology coordinators. Social engineering is a term commonly used to refer to manipulative human-human interaction, such as dishonest persuasion. An interesting statistic involves the number of teachers who may have been victims of social engineering; nine percent of the technology coordinators surveyed believed that their teachers had been victims of social engineering. Unlike many of the other security issues addressed in this study, social engineering as a security topic

has gone largely unnoticed in the press; this may be one of the reasons that teachers are generally unaware of social engineering ploys. However, while a relatively small number of teachers have been victims of some sort of social engineering ploy, it remains an important professional development topic.

Finally, from the technology coordinator's point of view, most teachers violate copyright law even if they are aware of it; however, the teacher survey indicates that teachers may not completely understand specific principles of fair use. Roughly one-third of the participating teachers were interested in professional development opportunities regarding copyright and fair use, which supports this idea.

It is imperative that teachers and support staff are provided with appropriate professional development opportunities so that they can effectively and efficiently protect themselves, their students, and their schools. As this study illustrates, teachers are willing to explore these professional development opportunities, specifically on topics such as copyright, software and Internet issues, FERPA compliance, and file management and backup; interestingly enough, these same topics have also been identified by technology coordinators as topics that teachers need to learn more about. For many of the topics, professional development should balance background information on why security measures are necessary with specific procedures.

The sample sizes for this study were relatively small, making it difficult to assume that the sample is representative of the larger K-12 population. Nonetheless, as exploratory work it serves to illustrate potential problems and opportunities in the realm of information security in K-12 schools. K-12 schools are part of a wider, global network that will continue to introduce a range of threats and vulnerabilities to K-12 systems, the information that resides on the systems, and the users that interact with the systems.

REFERENCES

CERIAS K-12 Outreach Program (2003). K-12 security assessment pilot program: *Overall findings and recommendations*. Retrieved March 26, 2004 from http://www.cerias.purdue.edu/education/k12/securing_k12/school_vulnerability_assessments.pdf

Computer Security Institute, (2002). 2002 CSI/FBI Computer Crime and Security Survey. Retrieved on July 1, 2003 from http://www.gocsi.com/press/20020407.html

Consortium for School Networking, (2004). CyberSecurity for the Digital District. Retrieved on June 26, 2003 from http://securedistrict.cosn.org/

Creswell, J. W. (2002). *Research design: Qualitative, quantitative, and mixed methods Approaches* (2nd Ed.). Beverly Hills; Sage, CA.

International Standards Organization. (2000). ISO 17799: Information Security Management. Retrieved on July 1, 2003 from http://www.iso.ch/

Schneier, B. (2000). *Secrets and lies*. Digital Security in a networked world. Wiley Computer Publishing; New York.

President's Critical Infrastructure Protection Board, (2002). *The National Strategy to Secure Cyberspace*. Retrieved on June 26, 2003, from http://www.whitehouse.gov/pcipb/.

U.S Department of Education, National Center for Educational Statistics. Internet Access in Public Schools and Classrooms: 1994 – 2002, NCES 2004-011, by Anne Kleiner and Laurie Lewis. Washington, D.C: 2003.