State of K12 Cyberethics, Safety and Security Curriculum in U.S.: 2010 Educator Opinion

STAYSAFEONLINE.org
National Cyber Security Alliance

Davina Pruitt-Mentle, Ph.D.

Educational Technology Policy,
Research and Outreach

February 15, 2010

National Cyber Security Alliance
NCSA
1010 Vermont Ave., NW
Suite 821
Washington, DC 20005
Email: info@staysafeonline.org

Educational Technology Policy
Linking Research to Practice
Research and Outreach

About NCSA

The National Cyber Security Alliance is a nonprofit organization. Through collaboration with the government, corporate, nonprofit and academic sectors, the mission of the NCSA is to empower a digital citizenry to use the Internet securely and safely protecting themselves, the networks they use, and the cyber infrastructure. NCSA works to create a culture of cyber security and safety through education and awareness activities. Visit www.staysafeonline.org for more information. Visit www.staysafeonline.org for more information. Friend us on Facebook and follow @staysafeonline on Twitter.

About Stay Safe Online

StaySafeOnline.org is the National Cyber Security Alliance's Website. Content on the Website is developed in cooperation with many of our partners including government, industry, non-profit and education partners. Since our goal is increased education about and adoption of cyber security practices, all of the content found at StaySafeOnline.org may reproduced, if provided for free, to educate the public on good cyber security and safety practices.

About ETPRO

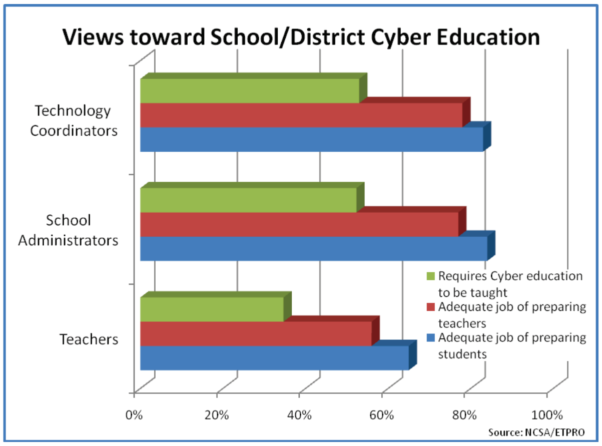
Educational Technology Policy, Research and Outreach, a research and development organization headquartered in Maryland, connects educational technology policy and research to instructional practice. ETPRO efforts draw from over two decades of experience in the educational community including more than a decade of experience in evaluating both formal and informal educational programs at the K-16 level, and nine years conducting educational technology policy analysis. ETPRO's understanding and insight into the fundamental gap between technology use and understanding of proper practices brought it to the forefront of research, program evaluation and development of Cyberethics, Cybersafety, and Cybersecurity (C3) initiatives.

EXECUTIVE SUMMARY

On behalf of the National Cyber Security Alliance (NCSA), Educational Technology Policy, Research and Outreach was engaged to provide detailed insight into important trends and opportunities emerging in the K12 classroom setting related to Cyber Ethics, Safety and Security topics. Zogby International conducted a hybrid telephone/online survey with 1,003 teachers, and telephone interviews with 400 administrators and 200 technology coordinators from U.S. schools who offered their opinions about the state of C3 education. The 2010 *Cyber Ethics, Safety and Security Survey,* an extension of *the 2008 National C3 Baseline Study*, finds more than half of administrators and technology coordinators agree their school/school district requires Cyber Ethics, Safety and Security curriculum be taught in the classroom setting. However, a third of teachers have not taught any topics related to Cyberethics in the past 12 months and more than 4 out of every 10 teachers have not taught any topics related to Cybersafety or Cybersecurity in the past 12 months. More than half of school administrators are more likely to think teachers/schools are primarily responsible for teaching children the content, compared to almost three quarters of teachers who feel parents are responsible for teaching children to use computers safely and securely. However, seven in ten teachers think Cyberethics, Cybersafety and Cybersecurity training should be a high priority in their professional development needs.

Among the findings:

- Nearly all technology coordinators (100%), school administrators (97%), and teachers (95%) agree Cyberethics, Cybersafety, and Cybersecurity curriculum should be taught in schools.
- More than half of schools/school districts require content coverage in Cyber Ethics (52%), Safety (57%) and Security (50%).
- Large discrepancies are revealed throughout the 2010 poll between perceptions of administrators and technology coordinators, and teachers.
- Teachers (72%) and technology coordinators (58%) are most likely to think parents are primarily responsible for teaching children to use computers safely and securely, while school administrators (51%) are most likely to think teachers/schools are primarily responsible for teaching children the content.

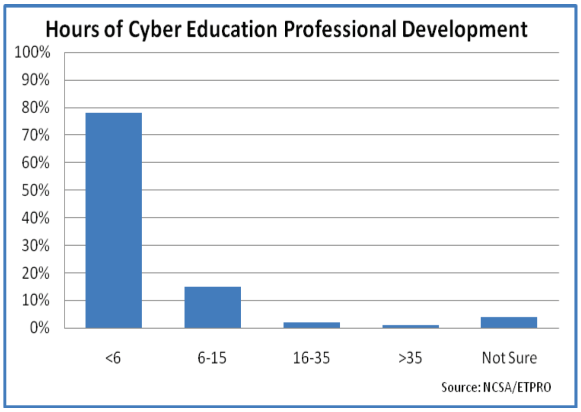


Source: NCSA/ETPRO

- According to all three groups filtering (95%), along with acceptable use policies (89%) and blocking (90%) continue to be the primary means for schools/school districts to ensure appropriate use of technology and the Internet.
- Fifty percent of teachers feel prepared to discuss cyberbullying, however 26% shared they were overall not prepared to talk about the subject.
- School administrators (66%) are more likely than teachers (40%) to be prepared to talk about strategies to protect personal information in online environments.
- A third of teachers (32%) have not taught any topics related to Cyberethics in the past 12 months. More than 4 out of ever 10 teachers have not taught any topics related to Cybersafety or Cybersecurity in the past 12 months.
- Twelve percent of teachers have talked about hacking, 33% discussed social networking sites, and 25% have taught about the importance of changing passwords in the last 12 months.
- Thirteen percent of teachers have discussed with their students the importance of Internet security to

the economy, and 8% have discussed with their students the importance of Internet security to national security in the last 12 months.

- Breaking down the educator group by type, the data show that technology teachers and media specialists feel better prepared than content teachers to discuss C3 topics.
- Over three quarters of teachers have spent less than six hours on any type of professional development education related to Cyberethics, safety, and security within the last 12 months.
- Local in-house workshops (73%) are the preferred method of technology coordinators to provide training to staff.
- Seven in ten (69%) teachers feel that Cyberethics, Cybersafety, and Cybersecurity professional development is a priority, and over 60% of teachers, administrators and technology coordinators are interested in training or receiving materials about cyberethics, safety and security issues.



Source: NCSA/ETPRO

- As revealed by school administrators and technology coordinators, more than half of schools make use of external Internet safety materials (56%). However, a combination of external and in-house materials (42%) or internal in-house curricula alone (23%) are the main sources of instructional cyberethics, safety and security content.

Since the 2008 Baseline Study, the awareness of Cyber Ethics, Safety and Security issues has clearly grown. Almost universally, the educational community believes these topics should be taught in schools, and the number of schools with policies that require coverage of this important subject matter has also increased. However, outside of these policy requirements, instructional activities do not necessarily align. There is focus on the technical solutions rather than instructional ones as schools use filtering and blocking as the primary mechanism for safety. Comprehensive coverage of diverse ethics, safety and security topics is necessary to help educators and students navigate the constantly changing ethical, safety and security demands brought about by emerging technologies and the evolving uses for current technologies. At this point teachers can only include selective topics in their classroom instruction due to the need for more professional development and resources. All teachers, technology coordinators and administrators agree professional development related to these areas is a high priority which reflects what teachers shared in 2008. Limited funding for efforts outside building achievement scores is probably the source of the limited access educators have to cyber related professional development.

Davina Pruitt-Mentle, PhD is the Executive Director of Educational Technology Policy, Research and Outreach

METHODOLOGY

Teachers:

Zogby International was commissioned by the National Cyber Security Alliance to conduct a hybrid telephone/online survey of teachers. Interviews were conducted between December 29, 2009 and January 11, 2010, with 335 completed interactively and 668 conducted by telephone for a final total of 1,003 teachers.

Telephone samples were randomly drawn from telephone CDs of national listed sample. Zogby International surveys employ sampling strategies in which selection probabilities are proportional to population size within area codes and exchanges. Up to six calls are made to reach a sampled phone number. Cooperation rates are calculated using one of AAPOR's approved methodologies[1] and are comparable to other professional public-opinion surveys conducted using similar sampling strategies.[2]

Separately, a sampling of Zogby International's online panel, which is representative of the adult population of the U.S., was invited to participate.

The margin of error is +/-3.2 percentage points. Margins of error are higher in sub-groups.

School Administrators and Technology Coordinators:

Zogby International also conducted a survey of administrators and technology coordinators working in K-12 schools. Fieldwork was conducted between January 4, 2010 and January 15, 2010. The administrator sample included 400 interviews with approximately 21 questions asked. Samples were randomly drawn from a list of a purchased K-12 administrator's database. The IT professionals sample was 200 interviews with approximately 21 questions asked. Samples were randomly drawn from a list of contacts supplied by the NCSA. Zogby International surveys employ sampling strategies in which selection probabilities are proportional to population size within area codes and exchanges. Up to ten calls are made to reach a sampled phone number. Cooperation rates are calculated using one of AAPOR's approved methodologies[3] and are comparable to other professional public-opinion surveys conducted using similar sampling strategies.[4]

DEMOGRAPHICS

For each respondent, questions regarding school type/level, and population of the local area were asked. Additionally, for teachers, they were asked whether they were content teachers, technology teachers, media specialists, or other. The demographic tables below show the cross-section of educators obtained. Several items are worth noting. For school administrators, a large number (33%) of respondents were at the district county level. These respondents are well in tune with what would be happening at the district level. Additionally, the teacher group surveyed has a higher percentage of high school teachers (36%) than revealed by the National Center for Education Statistics, Common Core of Data (CCD), "Public Elementary/Secondary School Universe Survey," where it was estimated that 23.7% of schools in the U.S. are secondary schools. Thus, the survey may have a bias toward the opinions of high school teachers; however, since advanced cyber

[1] See COOP4 (p.38) in Standard *Definitions: Final Dispositions of Case Codes and Outcome Rates of Surveys*. The American Association for Public Opinion Research, (2000).

[2] *Cooperation Tracking Study: April 2003 Update*, Jane M. Sheppard and Shelly Haas. The Council for Marketing & Opinion Research (CMOR). Cincinnati, Ohio (2003).

[3] See COOP4 (p.38) in Standard *Definitions: Final Dispositions of Case Codes and Outcome Rates of Surveys*. The American Association for Public Opinion Research, (2000).

[4] *Cooperation Tracking Study: April 2003 Update*, Jane M. Sheppard and Shelly Haas. The Council for Marketing & Opinion Research (CMOR). Cincinnati, Ohio (2003).

topics are more aligned with high school, this bias should not harm the relevancy of the information.

The survey also includes percentage wise, a larger cross-section of public schools than private schools. Nationwide, the Council for American Private Education estimates 25% of schools, and 11% of students in the U.S. to be in private schools. There were no private/parochial school administrators included in the survey, and only 8% of teachers came from this group. Thus, results may be more applicable to public schools than private.

A third (32%) of technology coordinators and a quarter each of teachers (26%) and school administrators (25%) report that a rural or farming community best describes their location, while another quarter each of technology coordinators (24%) and school administrators (23%), along with a fifth (21%) of teachers say a small town with a population of less than 25,000, but more than 2,500 best describes their location.

Population Density of School Location

	Teachers	School Administrators	Technology Coordinators
Rural or farming community	26%	25%	32%
Small town (population of less than 25,000 but more than 2,500)	21%	23%	24%
Mid-size city (50,000 to 250,000 people)	17%	13%	13%
Large city (over 250,000 people)	11%	11%	7%
Large town (population of more than 25,000 but not a suburb of a larger city)	9%	11%	11%
Suburb of a large city	9%	8%	10%
Suburb of a mid-size city	8%	8%	4%
Other/Not sure	1%	1%	--

Seven in ten (72%) respondents to the teacher survey report content teacher is the best title to describe themselves, while six percent identify themselves as either technology teachers or media specialists. A large group (22%) stated that none of these titles described their role.

Teacher Type (Teacher Survey Only)

Title that best represents you (Teacher Survey)	
Content Teacher	72%
Technology Teacher	4%
Media Specialist	2%
Other	22%

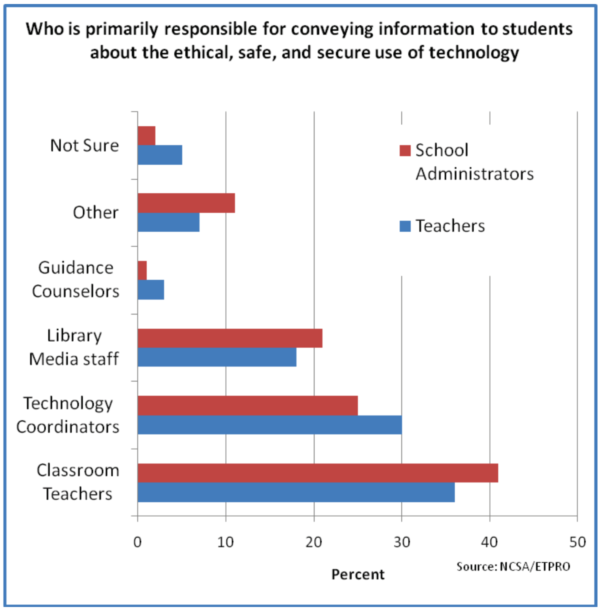
School Type

	Teachers	School Administrators	Technology Coordinators
Elementary school	38%	46%	51%
High school	36%	43%	27%
Middle/junior high school	25%	49%	37%
Kindergarten	11%	32%	25%
District/County level	10%	33%	17%
Private/Parochial school	8%	0%	16%
Pre-Kindergarten	6%	22%	12%
Charter school	3%	4%	3%
Independent school	3%	5%	6%

Note: Respondents can be in multiple categories, so columns do not total to 100%

INTRODUCTION

Technology, and the opportunities and dangers it presents, are ever growing and changing. For example, we have seen the growth of computer and cell phone access which has been coupled with the growth of cyberbullying and sexting. In 2009, 93% of teens 12-17 regularly went online compared to a little more than 70% in 2000 (Lenhart, 2009b). The use of social networking


Who is primarily responsible for conveying information to students about the ethical, safe, and secure use of technology

Source: NCSA/ETPRO

sites has more than quadrupled in the past several years, Facebook reached 400 million users as of February 5, 2010 (Zuckerberg, 2010), and the use of cell phones to call or text friends has replaced landlines and instant messaging since 2006 (Lenhart, 2009b). The greatest increase in cell phone access between 2004 and 2009 came in younger children; a Pew Internet study of 12 and 17 year old children reported a 40 percent growth in cell phone ownership in 12 year olds (from 18% to 58%). The majority of 17 year olds (83% vs. 64% in 2004) also reported owning their own phone in 2009 (Lenhart, 2009). *The Online Victimization of Youth: Five Years Later* study reported that sexual material and cyberharassment increased in the time between the 2001 and 2006 studies (Wolack et al., 2006). Recent figures on sexting indicate that 4% of 12-17 year olds have sent a sexually suggestive picture of themselves; however, 15% of the same age group admitted to receiving suggestive pictures (Lenhart, 2009a).

There has also been an exponential growth in cybercrimes reported to the FBI since 2000. In 2000, 16,383 incidents were reported; in 2008 the number grew to 275,284. The most frequently reported cybercrime was credit/debit card fraud; however, intrusion, spam, and child pornography were also frequently reported. Commercially, losses attributed to computer security issues averaged more than $230K per organization in 2008 with over 60% of the losses being attributed to non-malicious actions by insiders (Robinson, 2008). The FBI, CERT, and (ISC)^2 prioritize education and awareness before technical interventions in protecting users and infrastructure.

Indeed, increasing public awareness about cyberethics, safety and security in the United States is one priority spelled out in the President's 60 Day *Cyberspace Policy Review* (2009). As referenced in the report, "The United States should initiate a K-12 cybersecurity education program for digital safety, ethics, and security; expand university curricula; and set the conditions to create a competent workforce for the digital age (p.13)." The report goes on to state, "The Federal government, with the participation of all departments and agencies, should expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy. Existing programs should be evaluated and possibly expanded, and other activities could serve as models for additional programs (p.14)."

Understanding the state of cyber education policies and programs in the U.S. educational setting is essential for those concerned about promoting responsible behavior with digital media. This poll is a snapshot in time, providing a factual description of the state of cyberethics, safety, and security educational awareness policies and practices currently taking place in the U.S. K-12 educational settings. Survey questions focus on:

- What is the perceived importance of C3 content for U.S. K-12 school programs?
- What is the nature and extent of C3 learning in U.S. K-12 schools?
- Who are the major providers of C3 content in U.S. K-12 schools?
- What content is being delivered to educators, and how is it being taught?

Results from this poll enable us to better understand educators' perceptions about C3 content, the nature and extent of current policies and curricula, who currently teaches the content and how teachers are prepared to teach this topic. In sum, it provides a detailed look at current K12 educational patterns related to Cyber Ethics, Safety and Security educational programs.

State of Affairs

In 2008, a study was conducted to explore the nature of Cyberethics, Cybersafety, and Cybersecurity educational awareness policies, initiatives, curriculum, and practices taking place in the U.S. public and private K-12 educational settings. *The 2008 National C3 Baseline Study* established baseline data on the awareness, content, comfort, professional development and educational programs on C3 taking place throughout the U.S.

Across the board, findings found the state of C3 education to be incomplete. Content was limited; teachers did not feel comfortable with the topics; standards which set the stage for content coverage only peripherally discussed the issues; and little to no training was available for educators surrounding these topics.

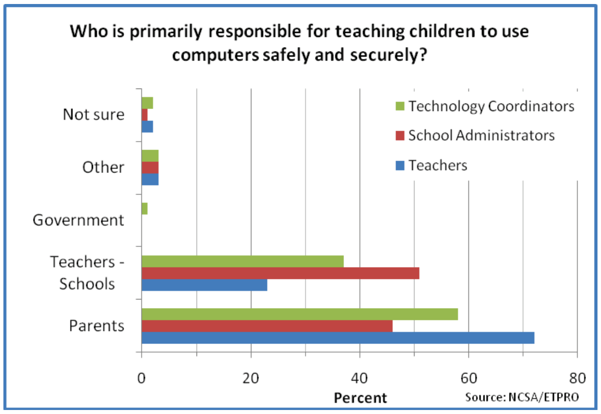
Several things have changed since this study: the International Society of Technology in Education (ISTE) National Educational Technology Standards (NETS) standards for teachers, students and administrators have been refreshed; awareness by Internet safety curriculum providers has resulted in more updated content that is research-based, less focused on stranger danger campaigns, and includes cybersecurity topics; states include cyber citizenship awareness topics in their technology standards and/or state curriculum (or portions of them); and the passage of the *Broadband Data Improvement Act: Protecting Children in the 21st Century* requires schools to teach Internet Safety. Even with these changes, continuous growth in digital media content and new technology such as social networking result in new challenges to provide appropriate and timely training.

The dynamic cyber environment requires regular research in a flexible schema which is updated to investigate status of Cyberethics, Safety and Security education. This poll helps us meet this challenge by broadening our understanding of these topics in K12 schools, and establishes a basis and context for discussions within the educational and policy communities.

What is the perceived importance of C3 content for U.S. K-12 school programs?

Nearly all technology coordinators (100%), school administrators (97%), and teachers (95%) surveyed agree that Cyberethics, Cybersafety, and Cybersecurity curriculum should be taught in schools.

Teachers (72%) and technology coordinators (58%) are most likely to think parents are primarily responsible for teaching children to use computers safely and securely, while school administrators (51%) are most likely to think teachers/schools are primarily responsible for teaching children the content.



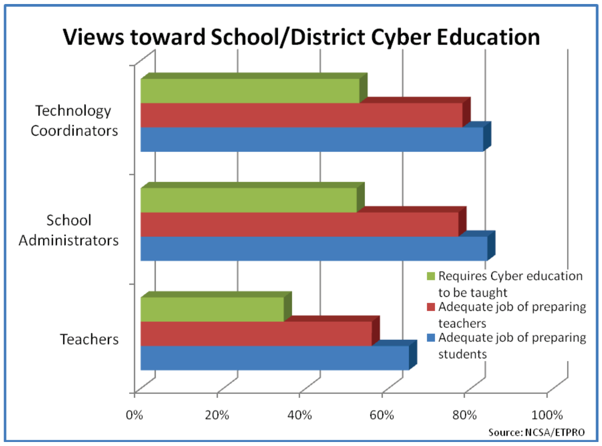
When prompted to choose who is primarily responsible for conveying information to students about ethical, safe and secure use of technology in schools, according to both teachers and school administrators, classroom teachers (36% vs. 41%) and technology coordinators (30% vs. 25%) are the two sources that come out on top.

Since 2008, more schools/school districts have recognized the importance of C3 topics, and as a result, the requirement for content coverage has risen in all three areas. In 2010, technology coordinators report that 52% of schools/school districts require content coverage in Cyber Ethics, 57% require Cyber Safety, and 50% require Cyber Security.

What is the nature and extent of C3 learning in U.S. K-12 schools?

Large discrepancies are revealed throughout the 2010 poll between perceptions of administrators and technology coordinators, and teachers. For example:

- School administrators (84%) and technology coordinators (83%) are more likely than teachers (65%) to agree their school/school district does an adequate job of *preparing students* regarding cyberethics, safety, and security issues.
- Technology coordinators (78%) and school administrators (77%) are more likely than teachers (56%) to agree their school/school district does an adequate job of *preparing teachers* to discuss with students topics regarding cyberethics, safety, and security issues.



Source: NCSA/ETPRO

- More than half of administrators and technology coordinators agree their school/school district *requires* cyberethics, safety and security curriculum be taught in the classroom setting, compared to only a third of teachers who agree.

Student Preparation Satisfaction

My school/school district does an adequate job of preparing students regarding Cyberethics, safety, and security issues	
	% Agreeing
School Administrators	84%
Technology Coordinators	83%
Teachers	65%

Population density comparison data provided interesting results. Teachers from school districts in large cities and in suburbs of large cities revealed they felt students were less adequately prepared for C3 topics and teachers were not adequately trained to teach students about C3 topics than their peers in small/large towns and rural or farming communities. Additionally, their districts were less likely to require cybersecurity curriculum in the classroom.

Teacher Perspectives Toward Cyber Education Preparedness by Local Population Density

Teachers feelings toward student preparation (Percent indicates agreement)	Overall	Rural or farming community	Small town	Large town	Mid-size city	Suburb of a mid-size city	Large city	Suburb of a large city
My school/school district does an adequate job of *preparing students* regarding Cyberethics, safety, and security issues.	65%	72%	69%	62%	61%	64%	53%	60%
My school/school district does an adequate job of *preparing teachers* to discuss with students topics regarding Cyberethics, safety, and security issues.	56%	63%	60%	60%	50%	45%	46%	50%
My school/school district *requires* Cyberethics curriculum be taught in the classroom setting.	34%	38%	36%	31%	33%	28%	29%	32%

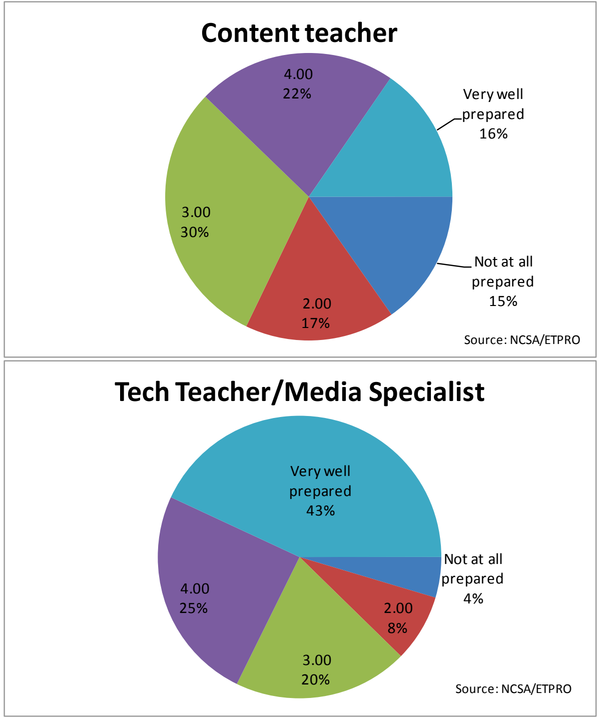
Important, albeit subjective, questions were asked of teachers regarding how well prepared they were to instruct in certain areas. Human nature suggests that we are more likely to teach in an area of strength, so this question can be a leading indicator to student instruction. Poll findings revealed an increase since the baseline study, with about half of the teachers indicating they feel prepared to discuss cyberbullying. Similarly, the percent of teachers who feel prepared to discuss strategies to protect personal information in online environments (i.e., updating anti-virus protection, recognizing phishing and pharming scams, how to reduce malware etc.) was 40%.The percent of teachers who feel prepared to discuss with students how to automate data backups was 26%. A little less than half of teachers polled (48%) responded they were prepared to discuss the dangers of sexting or sending sexually explicit messages or photos by mobile devices with their students.

The poll also asked school administrators about their perceived preparation. Data indicate school administrators (66%) are more likely than teachers (40%) to be prepared to talk about strategies to protect personal information in online environments, with nearly two-fifths of school administrators (37%) reporting they are very well prepared.

Further data analysis by educator role shows that technology teachers and media specialists felt better prepared than content teachers to talk about strategies to protect personal information in online environments.

Over the past year, many state and national efforts have spotlighted bullying and cyberbullying therefore, it is not surprising to see that a majority of school administrators (75%) indicate they feel prepared to talk about the subject, with about half (45%) of school administrators saying they are very well prepared. Within the teacher group, only 22% of content teachers felt very well prepared to discuss cyberbullying, while 51% of technology coordinators and media specialists felt very well prepared to discuss cyberbullying.

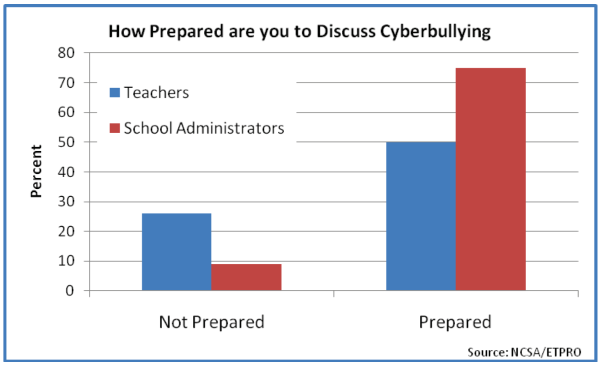
How prepared you are to talk about strategies to protect personal information in online environments (updating anti-virus protection, recognizing phishing/pharming scams, how to reduce malware, etc.)?
[scale of 1 to 5, 1 : not at all prepared, 5 very well prepared]



Source: NCSA/ETPRO

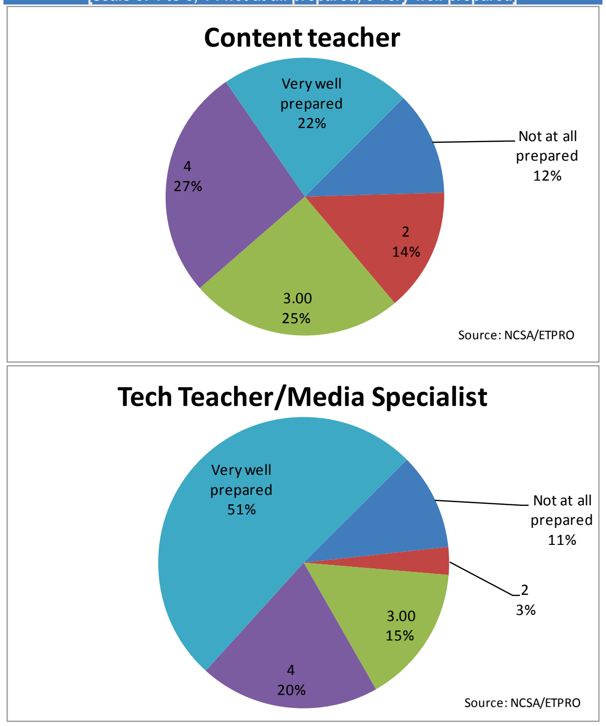
Source: NCSA/ETPRO

School administrators (66%) are also more likely than teachers (48%) to feel prepared to discuss sexting or sending sexually explicit messages or photos by electronic devices and are almost twice as likely as teachers (49% vs. 26%) to be prepared to talk about how to automate data backups. Again, the content teacher trails technology teachers and media specialists in how well prepared they feel to cover these areas. Although not unexpected, this illuminates an area that may require additional attention.



Source: NCSA/ETPRO

How prepared you are to talk about Cyberbullying?
[scale of 1 to 5, 1 : not at all prepared, 5 very well prepared]



Content teacher

Source: NCSA/ETPRO

Tech Teacher/Media Specialist

Source: NCSA/ETPRO

Although teachers and administrators feel more prepared to teach C3 content than in 2008, they are only translating their knowledge to the classroom to a limited degree. Nearly one third of teachers (32%) indicated they have not taught any topics related to Cyberethics in the past 12 months. In addition, more than 4 out of every 10 teachers revealed they had not taught any topics related to Cybersafety or Cybersecurity in the past 12 months.

While all survey respondents almost unanimously agree that cyber curriculum should be taught in schools, it appears that Cyberethics, Safety, and Security topics are making it into the classroom at marginal levels. For example, only 12% of teachers talked with students about hacking, 25% taught about the importance of changing passwords, and 33% discussed social networking sites within the last 12 months. As the importance of the Internet grows in our everyday life and moves into every facet of the economy, we must make sure that all are contributing to making it safe and secure. Recent revisions to professional and student instructional technology and media standards, have made progress toward improving digital literacy by including awareness for understanding societal issues related to technology within their framework. However, very few teachers have discussed the importance of Internet security to the economy (13%) and national security (8%). Guidelines such as these rely on implementation by state and local school systems. In addition, these revisions may be too recent to appear in the data collected in this survey.

Teacher's Perceptions of Topics Taught

Which of the following topics have you taught in the last 12 months

Topic		2010
Cyberethics		
Hacking		12%
Plagiarism		56%
Downloading music and video		27%
None		32%
Cybersafety		
Not sharing info with strangers		39%
How to react to harassment		28%
What to do if someone posts inappropriately		23%
Dangers of social networking sites		33%
Sexting		22%
None		44%
Cybersecurity		
Antivirus		14%
Firewall		16%
Changing passwords		25%
Using spam filters		13%
Never sharing computer account		42%
Identify secure website		22%
Role of a secure Internet in our economy		13%
Role of a secure Internet in our national security		8%
None		43%

Comfort Level

How well prepared do you feel to talk about:

	Content Teachers		Tech Teachers/ Media Specialists	
	Very Well Prepared	*Prepared*	*Very Well Prepared*	*Prepared*
Cyberbullying	22%	27%	51%	20%
Sexting	26%	23%	43%	17%
Automate backups	11%	15%	41%	16%

Who are the major providers of C3 content in U.S. K-12 schools?

Many state education curricula and professional standards include Cyber Ethics, Safety and Security content, or at minimum selective topics. Technology coordinator data reveal about half of the schools/ school districts require content coverage in all three areas of Cyber Ethics (52%), Safety (57%) and Security (50%), while in 2008 only 18% of coordinators indicated that C3 topics were required. Although over half of school administrators and technology coordinators believe C3 content is required in the classroom, only on the order of one third of teachers agree with this statement.

Participants' Perceptions of Curriculum Requirement

My school/school district requires Cyber______ curriculum be taught in the classroom setting			
(% indicate agreement)	Technology Coordinators	School Administrators	Teachers
Ethics	52%	51%	34%
Safety	57%	54%	37%
Security	50%	52%	33%

Interestingly, according to all three groups, filtering (95%), along with acceptable use policies (89%), and blocking (90%) continue to be the primary means for schools/school districts to ensure appropriate use of technology and the Internet. Similar findings were found in the 2008 Baseline Study data.

How schools inform students and educators about responsible use

Large majorities of teachers, school administrators, and technology coordinators report that their school/school district use the following ways to inform students and educators about specific laws, policies and guidelines related to the ethical use of resources: modeling and encouragement of appropriate ethical behavior; acceptable use policies included in student and staff handbooks; presentation of copyright information at faculty meetings, in newsletters, and during staff development; copyright policies and procedures included in student and staff handbooks; and up-to-date file of copyright permissions, purchase orders, software licenses, or documentation, etc. to document legal compliance as ways to inform students and educators about specific laws, policies, and guidelines related to the ethical use of resources.

All three groups agree they are modeling ethical behavior. In addition, slightly more than half of school administrators (55%) and half of teachers (50%) say the provision of bibliographic citations is also used to inform students and educators about the ethical use of resources, while 55% of school administrators and technology coordinators report the presentation of copyright information at student presentations is also used. Almost half of all teachers and administrators surveyed agreed that their school posts copyright notifications on equipment.

How students and educators are informed about Cyberethics safety and security issues			
Topic	**Teacher**	**Tech Coord**	**Admin**
Modeling and encouragement of appropriate ethical behavior among staff and students	78%	87%	88%
Acceptable use policies and procedures (that address ethical use of material) included in student and staff handbooks	78%	76%	84%
Copyright policies and procedures included in student and staff handbooks	66%	67%	73%
Presentation of copyright information at faculty meetings, in newsletters, and during staff development	63%	74%	55%
Up-to-date file of copyright permissions, purchase orders, software licenses or documentation, etc. to document legal compliance	54%	57%	56%
Provision of bibliographic citations	50%	55%	48%
Copyright notices on appropriate equipment throughout the building	48%	63%	48%
Presentations about cyberbullying at student sessions	44%	40%	40%
Presentation of copyright information at student presentations	41%	55%	55%
Presentations about consequences of sexting or sending sexually explicit messages or photos at student sessions	38%	34%	32%
Presentations about protecting, identifying, and responding to cybercrime (i.e. identity theft, spam, phishing, and pharming scams, malware) at student sessions	31%	27%	30%

Consequences of sexting or sending sexually explicit message and photos are said to be presented to fewer than 40% of students and sharing information related to protecting, identifying and responding to cybercrime, is presented by fewer than one third of schools.

Type of Internet Safety Curriculum

As revealed by school administrators and technology coordinators, more than half of schools make use of external Internet safety materials (56% and 54% respectively). However, within these groups, most used a combination of external and in-house materials (42% and 39%) or internal in-house curriculum alone (23% and 27%) as the main source of instructional Cyber Ethics, Safety and Security content. Less than 10% of either group shared that an external Internet safety curriculum was used exclusively to meet their needs.

Of those who indicated they used an external Internet Safety content provider as part of their curriculum, two-fifths (39%) of technology coordinators and a third (34%) of school administrators were not sure which curriculum they used, while 22% and 28% respectively did not use one of the four curriculums included in the poll.

Internet Safety Curriculum Choice

Which of the following is the primary Internet safety curriculum your school/school district uses?		
	School Administrators	Technology Coordinators
A combination of external Internet safety providers and in-house materials	42%	39%
An internal in-house curriculum	23%	27%
A combination of external Internet safety providers	9%	6%
An external Internet safety provider	5%	9%
Other	3%	9%
Not sure	19%	12%

External Internet Safety Curriculum

Percentage Whose Schools Use		
	School Administrators	Technology Coordinators
i-SAFE	16%	13%
NetSmartz	14%	17%
CyberSmart!	6%	6%
iKeepSafe	2%	3%
Other	28%	22%
Not sure	34%	39%

What content is being delivered to educators, and how is it being taught?

Similar to the 2008 Baseline Study findings, the 2010 poll data reveal a general discomfort and lack of Cyber Ethics, Safety, and Security fluency by educators, and limited professional development opportunities. This section examines how teachers currently learn more about these topics; what professional development is being provided to educators; and, what training and materials are required as perceived by educators, technology coordinators, and administrators.

A disconnect exists between teachers, and school administrators and technology coordinators about the adequacy of training in C3 topics. Technology coordinators (78%) and school administrators (77%) are more likely than teachers (56%) to respond that their school/school district does an adequate job of *preparing teachers* to discuss with students topics regarding cyberethics, safety, and security issues. Teachers (41%) are most likely to disagree as compared to technology coordinators (22%) and administrators (21%). This discrepancy may explain the limited amount of training teachers report.

Perception of Teacher Preparation

My school/school district does an adequate job of preparing teachers to discuss with students topics regarding Cyberethics, safety, and security issues	
	% Agreeing
School Administrators	78%
Technology Coordinators	77%
Teachers	56%

So what types of C3 training opportunities are offered and what is the amount of teacher education?

According to school administrators, school sponsored workshops or seminars (53%) and mandatory professional development days dedicated to these issues (33%) are the ways most educators learn about Cyberethics, Cybersafety, and Cybersecurity issues. However, technology coordinators feel that school sponsored workshops (46%) are the primarily means for training, but list one-to-one or group training dedicated to C3 topics as a close second (42%) method.

Similarly to 2008, over three quarters of teachers have spent less than six hours on any type of professional development related to cyberethics, safety, and security within the last 12 months. Several studies have shown the correlation between increased professional development intervention and positive pedagogical changes. Additionally, in a meta-analysis of the literature on professional development, Guskey and Yoon (2009) reported finding a positive relationship between professional development, which had 30 contact hours or more, and student outcomes. Interestingly, 55% of technology coordinators polled indicated they have spent less than six hours providing C3 in-service education to their school system educators, compared to 78% of teachers who indicated they had spent less than six hours of training on any of these topics.

Yet, an increasing percentage of teachers, 69%, feel that Cyberethics, Cybersafety, and Cybersecurity professional development is a priority, and as the previous study found, the majority of participants surveyed are interested in training or receiving training and materials related to these topics.

Professional Development

About how much time have you spent on training and/or continuing education for Cyberethics, Cybersafety, and Cybersecurity (Teachers Only)			
	In-Service	*On Your Own (Professional Meetings, Workshops, and Conferences)*	*College Credit*
Less than 6 hours	78%	76%	85%
6-15 hours	15%	14%	4%
16-35 hours	2%	3%	1%
More than 35 hours	1%	2%	1%
Other - Not Sure	4%	4%	9%

Large majorities of technology coordinators (65%), teachers (65%), and school administrators (60%) are interested in training or receiving materials about cyberethical issues, including promoting academic integrity, combating and detecting plagiarism, rules for copyright and downloading, and helping students evaluate online content. Additionally, large majorities of teachers (69%), technology coordinators (69%), and school administrators (65%) are interested in training or receiving materials about cybersafety issues, including safe and best practices in social networking sites, inappropriate content or danger signs of suicide, huffing, reporting, or next steps with suspected criminal activities on the Internet.

Teachers (68%) and technology coordinators (64%) are more likely than school administrators (56%) to be interested in training or receiving materials about cybersecurity issues, including phishing and pharming scams, hacking, malware, identity theft, and strategies to secure their computer.

Professional Development Interest

Percent interested in training or receiving materials about:			
	Technology Coordinators	Teachers	School Administrators
Cyberethical issues	65%	65%	60%
Cybersafety issues	69%	69%	65%
Cybersecurity issues	64%	68%	56%

Forty-three percent of technology coordinators indicate a high priority for regional, university, or conference workshops related to cyberethics, safety and security. However, according to technology coordinators, in-school district workshops (73%) should be of highest priority when it comes to professional development training in Cyberethics, Cybersafety, and Cybersecurity topics followed by online module (54%) delivery.

In summary, the 2010 Cyber Ethics, Safety, and Security Survey extended our understanding of the current state of cyber education in our schools. As with the 2008 Baseline Survey, this information serves as a sign post pointing to the destination we seek: a well-informed educational and student population that keeps their personal, school, and ultimately national information secure and safe using ethical behaviors. Given our current location as described by this survey, we make the following recommendations which help guide us closer to our destination.

Recommendations

Recommendations have emerged from the survey findings and reflect a review of the data merged with experience and discussions from local, state and federal agencies, business, educational institutions, and current research.

The issues of Cyberethics, Cybersafety, and Cybersecurity cut across multiple domains; education, government, and industry and are imperative to both our nation's success and infrastructure. The educational system alone cannot be the sole creator and dissemination mechanism for information. Cross domain partnerships are needed to leverage content expertise with pedagogically sound instruction. Technological change and accompanying best practices continue to change rapidly. In order to keep pace, schools should develop partnerships with other public and private sector entities to encourage transfers of knowledge around security and emerging technologies and to engage technology professionals in supporting the educational mission around cyber ethics, cyber safety, and cyber security. It is imperative that knowledge transfer occur to allow educators to understand this growing and dynamic area. Informal education opportunities can also aid in providing resources for classroom use.

General citizenship awareness and preparedness efforts in cyber education must include both parent and educator content. Schools often focus on the most popular topics "of the day". Recent efforts toward cyberbullying are a case in point. However, digital literacy encompasses engaging young people in learning about staying safe and secure online and participating responsibly in the digital community and is much more than simply cyberbullying or individual efforts to curb posting of inappropriate content. Schools should adopt a comprehensive framework to address Cyberethics, safety and security issues. Many cyber education topics are covered within single professional development sessions, hour long school assemblies or single classroom presentations. However, decades of research show that material is best retained if presented using multiple methods over time. Given the complexity and extent of knowledge in this area, as well as continual technological change, it cannot be covered sufficiently as currently implemented and must be modified to contain sequential revisit and refresh.

Teachers and school staff should model correct ethical, safe, and secure practices in the classroom. However, educators need to feel more comfortable with the information in order to model it successfully and correctly. Professional development is key to preparing classroom instructors to take advantage of the teachable moments that occur every day during their instruction. Regularly scheduled professional development will provide teachers with the awareness and a comfort level they need to integrate C3 content into their standard curriculum teaching and their everyday lives. The need for professional development has not changed since 2008—although an even greater percentage of survey respondents indicate it is a high priority.

Technology impacts multiple domains including behavior, psychological and physical health, academic performance and workforce skills. Efforts need to include a broader landscape of educational stakeholders within our professional development envelope. Education for a larger group of stakeholders should be considered; teachers, administrators, media specialists, technology coordinators, nurses, school psychologists, and counselors. In addition, training resources and activities for parents, law enforcement and informal organizations including internet safety providers should be created and made readily available to all who need them.

Cyber education is a shared responsibility. As the entire country increasingly works “on the web”, it is imperative we know how we can act ethically, safely and securely within this virtual world. To accomplish this mission, the public and private, school/industry partnerships are imperative to accomplishment of our ultimate goal, a safe and secure Internet for all to use.

References

Agatston, P. W., Kowalski, R., & Limber, S., (2007). Students' perspectives on cyber bullying. *Journal of Adolescent Health*, 41, S59–S60.

The Berkman Center for Internet and Society at Harvard University (2008). *Enhancing child safety and online technologies : Final report of the internet safety technical task force to the multi-state working group on social networking of state attorneys general of the United States.* Retrieved from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf

Council for American Private Education. (2009). *Statistics at a glance.* Retrieved from http://www.capenet.org/facts.html

Cyberspace Policy Review: Assuring a trusted and resilient information and communications infrastructure (2009). Retrieved from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

DeHue, F., Bolman, C. & Völlink, T. (2008). Cyberbullying: Youngsters' experiences and parental perception. *CyberPsychology & Behavior,* 11(2), 217–223.

Guskey, T. R., & Yoon, K. S. (2009). What Works in Professional Development? *Phi Delta Kappan,* 90 (7), 495-500.

Hinduja, S. & Patchin, J. W. (2009). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. Sage Publications (Corwin Press).

Lenhart, A., (2005). Protecting teens online. Pew Internet & American Life Project. Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2007/PIP%20Cyberbullying%20Memo.pdf.pdf

Lenhart, A., (2007). *Cyberbullying and online teens*. Pew Internet & American Life Project. Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2007/PIP%20Cyberbullying%20Memo.pdf.pdf

Lenhart, A, (2008). *Teens, Video Games and Civics*. Pew Internet and American Life Project. Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Teens_Games_and_Civics_Report_FINAL.pdf.pdf

Lenhart, A. (2009a). *Teens and Sexting*. Pew Internet & American Life. Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2009/PIP_Teens_and_Sexting.pdf

Lenhart, A. (2009b). *Teens and Social Media: An Overview*. Pew Internet & American Life. Retrieved fromhttp://www.pewinternet.org/~/media//Files/Presentations/2009/Teens%20Social%20Media%20and%20Health%20-%20NYPH%20Dept%20041009nnAMREVISE.ppt

National Center for Education Statistics. (2008). *Public elementary and secondary schools, by type and state or jurisdiction: 1990–91, 2000–01, and 2006–07*. Retrieved from http://nces.ed.gov/programs/digest/d08/tables/dt08_098.asp

Pruitt-Mentle, D. (2000). The C3 framework: Cyberethics, cybersafety and cybersecurity implications for the educational setting

Richardson, R. (2008). 2008 *CSI computer crime & security survey:* The latest results from the longest-running project of its kind, Computer Security Institute.

Ridout, V. J., Foeher, U. G., & Roberts, D. F. (2010). *Generation M2: Media in the Lives of 8- to 18-Year-Olds,* Kaiser Family Foundation

Roberts, Foeher, and Rideout (2005, March 9): *Generation M: Media in the lives of 8-18 year olds*. Kaiser Family Foundation. Accessed at: www.kff.org/entmedia/upload/Generation-M-Media-in-the-Lives-of-8-18-Year-olds-Report.pdf

Smith, S. D., Salaway, G., & Caruso, J. B. (2009). *The ECAR student of undergraduate students and information technology, 2009*. Boulder, CO: EDUCAUSE.

Wolak, J., Mitchell, K., & Finkelhor, D. (2006). *Online Victimization of Youth: Five Years Later*. National Center for Missing and Exploited Children. Retrieved from http://www.unh.edu/ccrc/pdf/CV138.pdf

Zuckerberg, M. (2010). *Six Years of Making Connections*. Facebook. Retrieved February 5, 2010 from http://blog.facebook.com/blog.php?post=287542162130