ETPRO – NCSA

2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study

October 2008

Conducted by:
Educational Technology, Policy Research, and Outreach
Davina Pruitt-Mentle, Ph.D.
www.edtechpolicy.org

for

National Cyber Security Alliance
www.staysafeonline.org

About the National Cyber Security Alliance
The National Cyber Security Alliance is a 501(c)(3) nonprofit organization. Through collaboration with the government, corporate, non-profit and academic sectors, the mission of the NCSA is to create a culture of cyber security and safety awareness by providing the knowledge and tools necessary to prevent cyber crime and attacks.

The National Cyber Security Alliance focus is Home Users, K-12 Educators, Small Businesses and Higher Education.

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.

Table of Contents

Foreword

Why study what schools are teaching to children about cyber crime and cyber security?

The answer is simple. We now live in the digital era and young people today will be the first to grow up with the Internet as an integral part of their lives. If we are going to so openly allow technology into our lives, we need to be sure that we are doing everything possible to teach children how to be safe and secure online. We need to provide a framework for young people to make good decisions about their online behavior and use this amazing technology responsibly. The bar should be set high with the goal of teaching cyber security, cyber ethics, and cyber safety until it becomes second nature – just like looking both ways before crossing the street or buckling seat belts in a car.

Children are connected to the Internet at home, at school and while they're on the go. They are shunning traditional communication methods and replacing them with instant and text messaging, they keep their friends posted on their activities and whereabouts with social networking, they play games against people across the globe, and they use the Internet to find and play music, watch movies and T.V. Teachers and parents need to find ways to make sure that young people have the tools in place and adopt the behaviors that can protect them.

Schools are a natural partner, along with parents and other youth-serving organizations, to teach cyber safety and cyber security. Responsibility to teach cyber security and safety stems from more than the traditional role schools have played in teaching safety to children. Schools have embraced the digital age as well through increasingly connected classrooms. Websites, listservs and other online tools are used for educational purposes and to keep students, parents and the community informed. As with any other classroom tool that poses potential risk (for example, from scissors to Bunsen burners), the first lessons should be about safety, and there should be a high level of confidence that students understand and have incorporated safe practices.

The goal of this study was look at how cyber safety, cyber security and cyber ethics issues are being addressed through the school systems. What topics are making their way into the classroom, who's teaching them and what tools are they using? How much time is devoted to these topics? Do teachers feel prepared to educate students about these issues? All teachers must understand how cyber security and safety fits within their classroom and their educational mission.

Digital literacy and 21st century technology skills are critical for the success of our children. This study creates a baseline from which we can measure our progress toward fully integrating age and developmentally appropriate cyber security, cyber ethics, and cyber safety education.

Michael Kaiser
Executive Director
National Cyber Security Alliance

1

Executive Summary

Introduction

Information technology has moved beyond a luxury solely for the business world, to become an integral part of the modern world; it is ubiquitous outside the formal classroom setting and is becoming a universal part of the K-12 environment. Technology clearly has brought a large number of positive effects to the educational community, including improved access to information, improved simulation capabilities, enhanced productivity, and a means to provide technology-based assistive support. In spite of these advances, technology has also brought challenges.

The power and possibilities that technology affords students comes with drawbacks if inappropriately used, whether such use is intentional or unintentional. Improving student knowledge and awareness of Cyberethics, Cybersafety, and Cybersecurity (C3)[i] concepts will provide them with the means to protect themselves, and will enhance the safety and security of our national infrastructure. Nurturing a C3 sensibility is every bit as important to our future as technology training. We need an integrated approach to develop a technologically-savvy workforce that understands the context and usage of digital communication as well as the nuts and bolts behind coding and functionality. The need for enhanced C3 instruction is evident by recent media focus on the topic. Cheating and ethics violations have been at the forefront of news in all facets of our society: the collapse of Enron and WorldCom corporations amid fraud and insider trading; numerous world sports figures including track and field, football, and baseball, have admitted to steroid/HGH use and/or gambling; author fabrication like James Frey's *A Million Little Pieces*; recent instances of students cheating on national SAT and AP exams; and students hacking into school systems to change grades or check on college acceptance status. Studies conducted over the past several decades indicate that 75-95% of college students have admitted to academic dishonesty.[ii] The Center for Academic Integrity reports that nearly 75% of high school students admit to academic dishonesty. A study conducted in 2000 and 2001, of 4500 students at 25 high schools, revealed that 74% admitted to cheating on a major exam.[iii] The National Crime Prevention Council reports that 43% of teens have been victims of cyberbullying in the last year.[iv] Ethical and moral decisions are occurring throughout the students' K-12 experience. In the 2005 Pew Internet and American Life report, *Protecting Teens Online*, 64% of online teens (ages 12-17) stated that they do things online that they wouldn't want their parents to know about, and 79% stated that they aren't careful enough when giving out information about themselves online.[v]

> *I believe all the issues discussed in this survey to be important and viable to the current canvass of our society. Students are becoming more and more engulfed in the cyber world and I fear that many of them are getting lost with no guidance for making correct choices. I applaud any efforts to make these issues a more important and frequently addressed concern of every student body across America!*
>
> (Northeast Educator)

Only recently has Cybersecurity awareness in the educational setting made it to the radar screen. Yet, the Federal Trade Commission (FTC) reports[vi] that for the seventh year in a row, identity theft tops the list of consumer fraud, and identity theft affects more than 10

million people every year, representing an annual cost to the economy of $50 billion dollars. Key findings from the 2007 CSI Computer Crime and Security Survey[vii] of IT security administrators (primarily government agencies and large corporations), found one-fifth suffered one or more kind of security incident and most from a "targeted attack." Financial fraud overtook virus attacks as the source of the greatest financial losses, and insider abuse of network or email edged out virus incidents as the most prevalent security problem. SANS[viii] listed web browser security, phishing and pharming attachments, and unencrypted laptops as just three out of twenty top security risks of 2007. For 2008, Georgia Tech's Information Security Center's top five emerging cyber threats included Web 2.0 and client-side attacks, targeted messaging attacks, Botnets, and threats to mobile convergence and Radio Frequency Identification systems.[ix] Google has stepped up its vigilance to report webpages containing malware. Google estimates that more than 1% of all search results contained at least one result that point to malicious content.[x] Denial of Service attacks, viruses, worms, Trojan horses, and computer fraud cost the country billions of dollars each year. In almost all cases, security recommendations for reducing the incidences of inappropriate or unsafe technology use included "user education" as a key solution.

The Survey Purpose and Process

In 2008, a survey was conducted to explore the nature of Cyberethics, Cybersafety, and Cybersecurity (C3) educational awareness policies, initiatives, curriculum, and practices currently taking place in the U.S. public and private K-12 educational settings. The study establishes baseline data on C3 awareness, which can be used for program design and as a foundation for future studies on either expanding particular subject areas or examining progress. This study used both qualitative and quantitative data and focused on:

- 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 is the perceived importance of C3 content for U.S. K-12 school programs?
- What content is being delivered to educators, and how is it being taught?
- What, if any, are the issues and barriers that impede the delivery of C3 content in U.S. K-12 school programs?

Data were gathered from a web-based survey, designed specifically for this project. Quantitative data were supplied by 1569 educators and 94 technology coordinators. Educators and local education agency (LEA) technology coordinators/directors also responded to an open-ended survey question allowing them to enter their own words in a text box. Qualitative data were collected by group and individual interviews. A total of 219 educators, local education agencies' technology director/coordinators, and state technology directors and/or their representatives participated in these focus groups. Arrangements were made for individual interviews for participants who wanted to share but were unable to make the focus group dates and times. Focus groups and interviews lasted between one hour and one hour and 20 minutes.

Key Findings

Across the board, this survey found the state of C3 education to be incomplete. Content is limited, teachers do not feel comfortable with the topics, and standards which set the stage for content coverage only peripherally discuss the issues. The following is a brief summary of survey results and includes some of the comments made by those surveyed and inter-

viewed. More detailed results of the survey can be found in Sections 3 to 5.

What's happening?

Currently, as perceived by educators, students receive little to no training on topics related to Cyberethics, Cybersafety, or Cybersecurity. Data indicate that states and local education agencies, as viewed by educators, place the majority of responsibility for conveying C3 content to students in the hands of educators. In practice, this responsibility is not necessarily translated to action; the content is not mandated and teachers feel unprepared to cover the topics. Some information, primarily ethical issues (copyright, downloading, and plagiarism), may be conveyed in Acceptable Use Policies (AUP) and/or student handbooks; however, comprehending the information is often left as an independent activity for the student. The policies are issued to the students and covered briefly at the beginning of the year. As discussed in Section 3 Table 3-8, the coverage of C3 topics included in AUP and student handbooks ranges from 27% up to 73.9%, depending on the subject. While some items are included within AUP and student handbooks, most discussions are limited to restrictions on the use of the school's IT infrastructure, and convey limited insights on the topics.

In some instances a limited view of Cybersafety is covered, generally from outside presenters. Participants indicated that presentations were usually stand-alone, often "one time" assemblies or events which were narrowly focused. Topics listed as being addressed specifically dealt with Internet predators, cyberbullying, precautions when using social network sites, and "stranger danger" campaigns.

Feedback indicates that schools/school districts often only address Cybersafety and Cybersecurity by limiting access and opportunity for violations: downloading is not allowed; students can only go to pre-selected and filtered websites; and/or no email access is allowed. This methodology relies on prevention rather than proactive promotion of C3 principles.

The education community today is driven by standards and assessments which are overseen by national, state, and local communities and are the basis for the curricula which are taught. The school day is busy, and teachers are reluctant to include any topics which are not specifically mandated or assessed. In the educational arena, standards serve as the guideline for content coverage. Technology standards are no exception. Education Week's *Technology Counts 2007 Report* indicated that the majority of states had adopted student technology standards—guidelines of what technology skills students should be aware of and what they should be able to do with technology. At the time of this study, all states except three had student technology standards in place. Out of the total, 16 states had integrated technology within the standards of other content areas, while 32 have adopted stand alone technology standards.[xi]

Although technology standards have been incorporated within state and local standards, these standards (as reported by survey respondents) predominantly focus on skills and are often silent on C3 issues. Standards do not seem to be covering the gamut of C3 topics, and do not keep up with changes. Since these issues are missing from standards, and are not being assessed, they are left out of classroom instruction. This is a recurring theme in the following comments offered by respondents. [See also Section 3]

> *Interesting to see how little we cover these issues in our district.* (Southwest LEA Technology Coordinator/Director)

I feel that these issues are viewed as "not important" by the district. They are more focused on teaching standard curriculums that pertain to state test scores. Cyber "anything" is viewed as non-relevant or not the district's responsibility to teach. (Northwest LEA Technology Coordinator/Director)

Interesting topics. Have not thought of them here at school. (Southeast Educator)

We do a pretty good job protecting students when they are on our own network within the school and address issues regularly dealing with acceptable use. We don't do well teaching them how to function safely and ethically OUTSIDE of the school environment. (Northwest LEA Technology Coordinator/Director)

We are developing lessons to incorporate this into content courses - but it needs to be required and monitored to ensure it is done. (Southeast Educator)

To the best of my knowledge we have NO program in place to educate adults or students in regards to cyber anything. (Southwest Educator)

In my elementary school we rarely discuss any of these topics. We use the computer mostly to do learning programs that are web-based or just loaded onto a specific computer. The students rarely use the web to do research or any other type of activity than the controlled, pre-selected programs. There is a strong filter that denies access to any blog site and most controversial sites. (Southwest Educator)

Very little information of this type is generally available to our school population, either teachers or students. (Northwest Educator)

While I can't say these things have occurred, I am aware my students are very active online. Therefore they must have been exposed to these kinds of things. By in large our district does little or no cyber education. (Southwest Educator)

I am not sure if students are getting C3 thru current ____ program--but most students appear not to be informed/aware of these areas of concern. (Southwest Educator)

I also am unsure as to how many of these issues are addressed in the schools. (Southwest Educator)

My school district does not really educate students on how to avoid all these Internet pitfalls, but rather, has a very thorough blocking practice which just doesn't let anyone get on anything, pretty much. (Southwest LEA Technology Coordinator/Director)

It seems to me that our district places a lot of emphasis on protecting users from inappropriate sites by blocking on a widespread basis. There is little or no curriculum dealing with teaching HOW to use technology appropriately. (Southwest LEA Technology Coordinator/Director)

How do English Language Learners protect themselves within cyberspace? My students have English as a second language and are just getting into computer technology but have not had training in their language. Is it available? (Southwest Educator)

Although I have used and have had children in my classrooms using computers for the past 20 years - these topics have received very little attention during technology training for classroom teachers. The

district does address some of these issues like safety, I think, but I don't know how. (Northwest Educator)

We have had many community workshops done by members of the local police department for parents, educators and students about the dangers of the Internet. (Southwest LEA Technology Coordinator/Director)

We have had the police department send in a speaker to discuss Internet safety with the students. (Northeast Educator)

I have taught an age appropriate Netsmartz safety lesson with my classes. (Northeast Educator)

Most of the focus has been on stranger danger…I do not think it works well with students (Northwest Educator)

I have partnered with the local police department to present _____ the last 5 years in one day workshops with all 6th graders in our school district. (Northwest Educator)

Who's Job is it?

Most survey participants indicated that C3 instruction has been placed in the hands of the educators. However, more than half of the educator respondents indicate they do not know how their school informs their students about a variety of issues including protecting, identifying, and responding to cybercrime (e.g. identity theft, predators, cyberbullying) and how to identify signs of documents and emails containing viruses. Additionally, many respond they do not feel that C3 topics should be their job; they feel it should be covered by parents. While the majority of educators perceive the task of covering ethical issues, such as plagiarism, to be the responsibility of the individual teacher, most feel the specifics of how to correctly cite and reference should be left in the hands of the media specialist or English teacher. Additionally, some educators have expressed frustration with policy enforcement related to issues such as plagiarism. They sometimes choose not to pursue violators, as parents defend their children and sometimes threaten legal action. School administrators are often reluctant to face such conflicts, and in many cases fail to support their teachers. [Section 3 and 4]

Much of what you survey here has nothing to do with teachers. It is the sole responsibility of students and parents. (Northeast Educator)

We deal more with parent education concerning these issues at our grade levels. (Southeast LEA Technology Coordinator/Director)

At first grade we mainly rely on parents and supervise them on the computer lab. (Northwest Educator)

We teach cyberethics and safety in the library but not all classes participate. (Southwest Educator)

Educating parents, not just educators needs to be considered since most of the inappropriate uses of technology occurs at home. (Northeast Educator)

Multiple methods of informing staff, students and parents are really needed (Northwest LEA Technology Coordinator/Director)

Preparation

This baseline survey sought to obtain information regarding knowledge gaps from the perspective of educators themselves. Do they feel

well enough informed to broach these subjects with their students? Are they able to model best practices in school and in their daily lives? How much exposure do teachers have to C3 related topics? The survey revealed educators feel ill-prepared to discuss C3 topics with their students. For Cybersecurity, 67% of respondents reveal they do not know how to update anti-virus, spyware, and anti-spam filters, and 52% do not know how to install operating system patches. Over 25% are not at all prepared to discuss basic Cybersafety issues such as what to do when receiving an unsolicited email. Surprisingly, 75% of educators feel uncomfortable discussing topics that have had significant public attention, such as cyberbullying. [Section 4]

> *I am not knowledgeable about any cyber topics.* (Northeast Educator)
>
> *I need to learn more on all these areas myself.* (Northwest Educator)
>
> *I thought I was kind of informed and up on things with regard to the Internet. I see I'm not at all up-to-date. I hope to share this with our tech director.* (Northwest Educator)
>
> *I have tried to understand cyberbullying by going to myspace.com but I didn't know what to do next.* (Northwest Educator)
>
> *After doing your survey I feel our staff/students do not know enough to protect them and it scares me.* (Southwest Educator)
>
> *I had no idea how much I didn't know. It's scary.* (Southwest Educator)

Training

In order to be prepared to address C3 issues, clearly educators need more training, either formal or informal. Survey results indicate that 90% of educators have received less than six hours of professional development on C3 topics in the last twelve months. Across the board, both educators and technology coordinators indicated a need for professional development and specified a preference for formal instruction, to be delivered as in-service training. Although not as desirable, for informal content delivery, 69.2% of educators, and 84.0% of technology coordinators indicated that they prefer digital media as the means to receive updated C3 information. [Section 5]

> *I feel very inadequate in this entire area and really need training.* (Northeast Educator)
>
> *More specific training and lesson objectives would be very helpful. I teach a computer technology class, and would find more information and/or training very useful*. (Southeast Educator)
>
> *I would really like to know more about this topic as I would like to work with older students and I am sure the problem is filtering to lower and lower grade levels.* (Southeast Educator)
>
> *This survey has caused me to think about all that I do not know. I hope that this survey results in cyber education for us educators!* (Southeast Educator)
>
> *I wish our district would provide much more of this type of training. It is important and a constant issue.* (Southeast Educator)
>
> *Without a personal interest in technology, it's difficult to get enough information through professional development work-*

shops to be ready to teach this information. (Northwest Educator)

I would like to have more training and a person within the school district to ask questions when I have concerns. (Southwest Educator)

I feel that in my position, Technology Integration at the school level, professional development on all 3 areas discussed here would be very beneficial. I would definitely take part in the opportunity if it were within a reasonable distance from my district--or IN my district. (Southwest Educator)

Our district staff has had very little technology training. (Northwest LEA Technology Coordinator/Director)

Concern, Need and Want

This C3 Baseline Survey was extensive and took participants a significant amount of time to complete. Despite the length, over 1600 educators and coordinators took the time to complete the online component. Additionally, 219 educators and local and state technology directors felt the topic important enough, and the aims of this study compelling enough to participate in focus groups for the survey. With all the demands on educators, this high rate of participation indicates the importance of addressing these topics more thoroughly. The words of the respondents transmit this message clearly.

This information all needs to be taught in the schools. I hope your project protects and informs students. (Northeast Educator)

I think our principals and district superintendent would also find this interesting. (Northeast LEA Technology Coordinator/Director)

I would like to see more of a nationwide initiative to help both educators and parents effectively monitor and guide children's digital communication. (Northeast LEA Technology Coordinator/Director)

This survey really made me want to ask administrators to start having programs on some of the cyber issues. (Southeast LEA Technology Coordinator/Director)

I would love to be able to better educate my students about all of the factors involved in C3. I definitely think this is a worth-while cause that needs to be addressed regularly and in-depth with students of all ages. (Northeast Educator)

I look forward to more information from you all and how I can take courses so I can share with the students and staff at my school. Will modules be available this summer? Will I be able to obtain continuing education credit for them? (Southeast Educator)

Thank you for being willing to conduct research; it is a very important endeavor. (Northwest LEA Technology Coordinator/Director)

Thanks for addressing the subject. (Northwest Educator)

This is a major issue in today's schools and it is important to develop programs so teachers know how to address these issues as they arise more and more frequently. (Northeast LEA Technology Coordinator/Director)

*Thanks for doing this survey. I am interested in your findings. Please send out any update e-mails to*_____ (Southwest LEA Technology Coordinator/Director)

I hope we participants will get to see the results of this survey. (Southwest LEA Technology Coordinator/Director)

Could you send the different categories you've used? (Southwest LEA Technology Coordinator/Director)

I would like to see a comprehensive plan addressing these issues in all schools. (Northwest LEA Technology Coordinator/Director)

Our school district would love to see the finished results of the survey. Is this possible? (Southwest LEA Technology Coordinator/Director)

With all the African money scams, social networks, IM & chat rms, it's clear that ethics, security, safety in cyberspace is a critical substantive area. (Southwest Educator)

Important topics. (Northeast Educator)

Conclusion

Past efforts in teacher education (both in-service and pre-service) have focused on teachers becoming knowledgeable about specific instructional technologies. Teacher technology training has been geared toward skills development, integration techniques and providing students with hands-on opportunities to use technology. However, this training has not been complemented by a similar national initiative on Cyberethics, Cybersafety, and Cybersecurity (C3) content. Teaching someone to drive is dangerous, unless you also teach them the rules of the road.

The call for a national focus impacting student and educator awareness and knowledge about C3 efforts has surged recently. State legislation has started to surface regarding Cybersafety awareness curricula (aka Internet safety) and cyberbullying. Schools are expanding their Acceptable Use Policies (AUP), PTA groups are hosting safety assemblies, and a plethora of Internet safety providers are engaged in awareness campaigns.

This survey attempted to better understand the level of Cyberethics, Cybersafety, and Cybersecurity educational awareness policies, initiatives, curriculum, and practices currently taking place in the U.S. public and private K-12 educational settings. The results provide valuable information into how state, regional, and local institutions are addressing C3 awareness. Input indicates that financial constraints, time commitments, bureaucratic processes, and an already over-packed curriculum agenda make it difficult for schools to successfully pursue C3 awareness efforts at the level they believe is necessary.

The National C3 Baseline Survey findings confirm the need for expanded C3 awareness and training in the educational community. This report describes how students receive awareness of Cyberethics, Cybersafety, and Cybersecurity topics in the educational setting, and what specific C3 topics are addressed currently by local educational agencies. Additionally, insight into educators' comfort levels, what topics present themselves in the general educational setting, type and time commitment devoted to professional development toward C3 topics, perceived needs of educators, and training preferences of educators was explored. If we look through the eyes of educators, we see little C3 content being shared with students. Content delivery is usually limited to one-day assemblies or individual lessons, and has primarily focused on "Internet safety," particularly emphasizing online predators, not sharing personal information and "stranger danger" campaigns. The majority of educators indicate a lack of confidence regarding Cyberethics, Cybersafety, and

Cybersecurity issues. They admit to a limited awareness about most C3 topics, and a lack of understanding that prohibits them from sharing information with students in either formal classroom lessons or in informal "teachable moments."

The survey results indicate that the majority of educators (67%) are interested in learning more about C3 topics, and that they feel Cyberethics, Cybersafety, and Cybersecurity are important and critical components to using technology appropriately. Overall, 53.8% of respondents indicate feeling ill-prepared to talk about C3 topics, and for most Cybersecurity topics, this rises to over 60%. Educators have a strong desire to learn more about all three areas, but feel they lack professional development opportunities. A comprehensive national approach to responding to the problem would aim to increase the training opportunities for educators, help bridge the gap between existing Internet awareness curriculum partners, call for expanding content to include a broader range of topics covered (particularly safety and security), and include program evaluation. More hands-on training opportunities for educators (not just resources and assemblies), and increased and on-going C3 awareness opportunities for youth throughout the K-12 experience would provide the comprehensive effort needed to close the gap between danger and knowledge.

As in all surveys, the conclusions are based on responses from a cohort, in this case participating educators. Although every effort was made to ensure a comprehensive set of educators were included in the survey, and the demographics in Section 2 indicate this to be the case, all surveys are limited by the true randomness of the participation and the extensibility of the survey to the population they represent. Based on the statistics of the survey, the interviews conducted, and the considerable experience of those conducting the study, the Educational Technology Policy Research and Outreach (ETPRO) organization believes the findings represent the true state of C3 awareness and education in the K-12 community.

Nothing in this report opposes the upwelling of educators and schools that are optimistically and effectively utilizing technology to promote learning, and engage and prepare students for 21st Century demands. However, this trend is complemented by an increase in complexity of C3 concepts, education, and enforcement. Therefore, this survey seeks to illuminate the gaps in current C3 policies, awareness initiatives, curriculum, and practices currently taking place in the U.S. public and private K-12 educational settings, and thereby help to move the agenda forward to address these problems in the early stages by informing national policymakers and key stakeholders. The survey will also hopefully promote further discussion and studies around these importance issues.

Recommendations

The recommendations, which follow, have emerged from the survey findings and reflect the data reviewed across multiple methodologies, merged with experience and discussions with a variety of educators and policy makers. These recommendations, although split into separate topics, overlap and reinforce each other, and together make a coherent policy framework to move aggressively forward to fill the C3 knowledge gap. Interested stakeholders may want to pick and choose which recommendations to implement. While this approach is understandable in light of today's funding constraints and full curricula, it should be used with caution. A concerted and united effort is essential to keep both our children and our national IT infrastructure safe and secure.

1. It Takes a Nation

> *We need to get the info to kids and parents. Radio and TV are often, unfortunately their main media source. We are remiss if we do not have this type of information broadcasted on these media.* (Northeast LEA Technology Coordinator/Director)

The issues of Cyberethics, Cybersafety, and Cybersecurity cut across education, government, and industry and are imperative to both our success and our security in the 21st Century. Providing information on these topics should not be considered the domain of only education. Resources, both content and funds need to be created through cross-domain partnerships. The businesses and industries that are driving technology advancements may be in the best position to provide the expertise in areas such as Cybersecurity. Funding for education is always under pressure, but due to the importance, funding should be created and allocated to assure these topics are appropriately addressed.

Impact requires a thrust using multiple means. Current efforts serve only as a bandaid, as most instruction is limited to policy statements in an AUP, signing a student code of conduct packet, or attending a one-day assembly. While better than nothing, decades of research show single-contact coverage, whether in the classroom or at one-time workshops for teachers, has little impact. Ongoing instruction is needed throughout the K-12 experience, starting in the early grades (many teacher respondents in this survey replied that C3 did not apply to them or their students since they were in elementary school), and continuing through high school. Middle school seems to be the end of many assembly programs on these topics. However, changes in technology, new means of plagiarism, and current safety and security concerns require ongoing and ever-evolving education, for students, educators, and parents.

In addition to classroom and teacher training, public awareness can be enhanced through efforts similar to the recent campaigns on green energy technologies and obesity. Public service announcements, talk shows, and news coverage are needed. Some instructionally-oriented cartoons talk about bullying. What about adding cyberbullying and other C3 topics? Perhaps some of the toys included in fast food meals could be developed to promote ethical, safe, and secure technology use. The possibilities are endless. Success can only result from multiple efforts that includes a variety of partners focused on the common goal– protecting our children and our nation, and preparing for tomorrow.

2. C3 Framework

Schools tend to pick and choose which C3 topics to teach, and often only talk about Cyberethics (e.g. plagiarism or cyberbullying). As revealed through survey findings, Cybersafety and Cybersecurity are virtually ignored in the educational setting, with the possible exception of a narrow focus on predators. Teaching to a C3 framework, where Cyberethics, Cybersafety, and Cybersecurity are taught as a whole, yet spotlighting each component's importance, provides the opportunity for more complete coverage. For example, one might need to learn security procedures to avoid having a computer vulnerable to an attack, as well as the ethical reasons not to hack into a computer to change grades. A separate focus gives rise to better appreciation of the appropriate uses of technology and does not lump the issues under a vague heading of *Internet safety*. By spelling out particular elements under each domain, educational institutions can better design and address critical content. Teaching the topics as one, through branding such as *digital citizenship* or *cyberawareness* makes it far too

easy to check off the topic as "covered," while only scratching the surface of individual domains.

3. Reinterpretation of Technology Standards

> *I consider myself basically computer illiterate. I am able to function with my in class computer to do attendance, input grades, check email, respond to email, and do basic Internet things like use a search engine. That is about it.* (Southeast Educator)

Standards for both students and educators set expectations. Standards are a good starting point for most subject areas, but the pace of change of technology creates a difficult challenge: how to keep standards up to date. Many technology standards were finalized several years ago before the advent of such issues as cyberbullying through text messages, test sharing through cell phone cameras, and identify theft through social networking sites. While standards are often broad-based to allow flexibility for evolving concerns, they need to be interpreted beyond the broad-stroke basics to make an impact. Perhaps the solution lies in more frequent updates to keep pace with change.

In addition, just because there are technology standards, teachers do not necessarily see it as their job to address them, integrated into their primary content area. All educators, administrators, specialists and teachers need to understand that teaching the technology standards is their responsibility.

4. Comprehensive, Systemic and Sequential Content Suggested

Educators know that topics such as fractions cannot be taught in a day. We know from decades of research that presenting material multiple times, in multiple ways, sequentially over time has the best return and maximum impact. Yet complex topics such as those capturedwithin Cyberethics, Cybersafety, and Cybersecurity are often covered in a single session. One-day assemblies are helpful, but the impact can be minimal given the plethora of content that needs to be covered and the difficulty in maintaining student focus in an assembly format. C3 topics need to be supported by more comprehensive content, taught using a variety of means over a longer timeframe, and refreshed as needs evolve.

5. Professional Development for Teachers a Must

> *Although technology has brought many positive things to education and has certainly enhanced our knowledge base and access to content, it has also brought many challenges that are not positive. As educators it is time we become technologically literate so that as a classroom teacher, we can embrace the power of the tools and use them instead of needing to spend all our time policing.* (Northwest LEA Technology Coordinator/Director)

Just because a topic area is listed in a standard does not mean teachers are prepared to teach it. Educators see the need, want to learn more, and are willing to put in the effort to learn the C3 content areas in order to pass the information on to their students. Providing curriculum for students is not enough. Many C3 issues did not exist when current educators were certified. Teachers need training on Cyberethics, Cybersafety, and Cybersecurity topics. It takes more than a workshop; schools need ongoing professional development which takes funding and expertise. Much of this expertise needs to come from outside the traditional "educational content domains." Additional funding and resources are needed both to provide content for local education agencies and to provide release time for teachers to be trained, at a time

where budgets for education are tight and funding for technology professional development is almost non-existent. If indeed national security, economic welfare of citizens, safety for youth, and a more ethical behavior across U.S. society is desired, then government, business/industry, and education need to team up to provide the needed information and resources to our teachers.

6. Don't Forget Informal Settings

> *I discuss C3 issues with girls in Girl Scouts from grades 1 - 5 as well.* (Northeast Educator)

Programs through Boys and Girls Clubs, 4-H, Boy Scouts, Girl Scouts, Parks and Recreation programs, after school programming, and before-and-after-care programs all provide additional learning opportunities for today's youth. These potential content providers should not be overlooked as additional intervention opportunities. However, program leaders (both volunteer and professional) will need instruction in C3 topics, and can benefit from prepared learning materials and lessons for their group. Once again, members of the business community can be tapped to provide expertise and enhance these teaching opportunities with real-world experience and lessons.

Some teachers feel that C3 education is the responsibility of parents. However, many parents are not prepared with the tools to deliver information in these areas. Many adults have only limited computer literacy; some lack the language skills or financial resources to overcome these limitations. Adults in informal settings can assist educators in providing the information for students and in helping parents understand the importance.

7. Policies, Processes and Procedures: Beyond Printed Text

The pace of change of technology requires continual updates to content and standards. The technology portions of Acceptable Use Policies (AUPs) and student handbooks need to be updated yearly. Instructional content needs to be updated to reflect best practices and lessons learned. However, if these were distributed in printed form, budgets would be strained to the breaking point. Instead, updating digital resources of policy, procedure, and content could allow for more frequent update. Incorporating comments from employees via listservs, blogs, and forums can enrich the dialogue and provide added value. Creating this dynamic digital information space may be critical to keeping up with technology changes.

Policies need to be reviewed to ensure that all employees (including teachers), students and parents understand them. The topics need to be covered more thoroughly than in a quick overview at the beginning of the year, when so many other things are distracting from the content. The topics need to be addressed in on-going instruction, both to ensure that students have the time and understanding to internalize the information and that new and transfer students receive the information. It is imperative that consequences are included and supported by administrators and school authorities (school boards and superintendent). Teachers sometimes feel unsupported and let ethical violations go rather than follow ill-defined and unenforced policies.

8. IT Departments are Not the Silver Bullet

Particularly in the area of Cybersecurity and, to a lesser extent, in Cybersafety, educators believe they have no role. Educators perceive that these issues are the domain of the Infor-

mation technology (IT) department, and ignore the topics both in the classroom and in their personal behavior. For example, they may assume all information on the school network is secure. Consequently, they use weak passwords, share their passwords, add unapproved software, or allow others to use their computers. Because they do not recognize the dangers, teachers sometimes lose the opportunity to instruct and guide. They miss the opportunity to inform students *why* it is ethically wrong to hack into the school computer to change grades. User education is critical and the perception that IT departments have "fixed" everything or blocked inappropriate content gives a false sense of security and unrealistic expectation. We need to make sure teachers understand their role in all C3 areas. The limited focus on filtering and blocking and establishing policies that say no blogs or social networks should give way to a broader focus on individual responsibility for using technology wisely. When students leave school they need to know what behaviors are appropriate and effective, so they are prepared for IT environments with less protection, and can act responsibly.

9. Recording and Reporting

Although documenting current efforts across a local education agency or state is difficult, there is a need to record and report C3 content being offered in schools. Improving learning includes understanding knowledge gaps, providing instruction, evaluating impact, and redesigning instruction. This process is aided by examining best practices rather than reinventing content in isolation. Analyzing existing content can also provide an opportunity for professional development. Prior to using existing curriculum in the classroom, teachers can assess whether they have the perquisite knowledge to teach it, if it is having an impact, why there are knowledge gaps for their students or in the curriculum, and prepare themselves and the content for better results.

ENDNOTES

---

[i] Cyberethics, Cybersafety and Cybersecurity, referred to as *C3*® is a Cyberawareness framework developed by Pruitt-Mentle, 2000. More about the development of the framework can be found in Appendix A. Other Terms and Acronyms can be found in Appendix B.

[ii] Goodwin, A. 2007. Exploring the Relationship between Moral reasoning and Student' Understanding of the Honor Code. Dissertation University of Maryland, 2007.

[iii] Center for Academic Integrity Study: Student Cheating in American High Schools. Donald L. McCabe May 2001 http://www.academicintegrity.org/

[iv] The National Crime Prevention Council Stop Cyberbullying Before It Starts. http://www.ncpc.org/resources/enhancement-assets/ncpc_cms/cyberbullying-pdf

[v] See Pew Internet and American Life Project Reports: Family, Friends and Community. http://www.pewInternet.org/PPF/r/152/report_display.asp

[vi] Federal Trade Commision 2007 Identity Fraud Survey Report. Javelin Strategy and Research http://www.privacyrights.org/ar/idtheftsurveys.htm#Jav2007

[vii] CSI 2007 Computer Crime and Security Survey. http://www.gocsi.com/

[viii] SANS Top 20 2007 Security Ricks. http://www.sans.org/top20/

[ix] The Georgia Tech Information Security Center (GTISC), Emerging Cyber Threats Report for 2008. http://www.gatech.edu/newsroom/release.html?id=1531

[x] Niels Provos, Anti-Malware Team. Google Online Security Blog. Feb. 11, 2008. All your iframe are point to us. http://googleonlinesecurity.blogspot.com/ http://googleonlinesecurity.blogspot.com/2008/02/all-your-iframe-are-point-to-us.html

[xi] Education Week's Technology Counts 2007, *http://www.edweek.org/ew/toc/2007/03/29/index.html*

2

Methodology and Demographics

Today's students are increasingly technology savvy and communicating and spend much time interacting socially online. In recognition of the importance of technology in our society, the No Child Left Behind (NCLB) Act of 2001 requires all students to be technology literate by the eighth grade. States are required to determine the number of students in public schools who are technologically literate and report the results to the U.S. Department of Education. Although select students may not be digitally literate as a consequence of digital inequity issues, others argue the new generation of students possesses an exceptional set of IT skills and knowledge. However, being *digitally literate* is not all inclusive. *Technology literacy*, as interpreted by some local education agencies and state departments of education, extends only to skills and does not focus on issues of ethics, safety, and security. In fact, limited efforts have dealt with preparing students to work with these three tenets in mind. Yet, numerous recent studies have spotlighted the issues.

- A study from the Center for Academic Integrity reported that nearly 75% of high school students admit to academic dishonesty.[xii]
- The National Crime Prevention Council reports that 43% of teens have been victims of cyberbullying in the last year.[xiii]
- The Pew Internet and American Life report, *Protecting Teens Online*, stated that 79% of online teens (ages 12-17) indicated they are not careful enough when giving out information about themselves online.[xiv]
- The Federal Trade Commission reports that in 2007, for the seventh year in a row, identity theft tops the list of consumer complaints at an estimated annual cost to the U.S. economy of $50 billion dollars.[xv]
- The 2007 McAfee-National Cyber Security Alliance Online Safety Study findings indicated fewer than one in four Americans surveyed were fully protected against viruses and malware. Just 22% had anti-spyware software installed, an enabled firewall, and anti-virus protection with a DAT file updated within the past week. Fifty-four percent of the respondents reported that they had had a virus on their computer, although the number may be higher, as 15% indicated they were not sure if they had a virus or not. Yet, 87% of Americans surveyed stored important personal information on their computer (e.g. financials, health records, personal emails) and 88% used their computers for sensitive activities such as banking and stock trading.[xvi]
- The 2007 CSI Computer Crime and Security Survey indicated insider abuse of network or email edged out virus incidents as the most prevalent security problem.[xvii]
- SANS listed web browser security, phishing and pharming attachments, and unencrypted laptops as just three out of twenty top security risks of 2007.[xviii]
- As the inclusion of multi-media rich content on the Internet grows, there is a similar explosion in the installation of browser plug-ins to view such content. These plug-ins by nature are often based on client-side web scripting languages, can be installed with very little (if any) interaction from the user, and may result in significant exploitable avenues for hackers.[xix]

Media coverage and study findings have caused a surge in Internet safety initiatives,

many targeting the K-12 educational arena. Assemblies, guest speakers, and Internet safety days/nights have become more commonplace. Several states have passed legislation[xx] requiring Internet safety be covered in schools. Others have legislation bills pending. But the question still remains: What Cyberethics, Cybersafety, and Cybersecurity (C3) lessons, curriculum, and content are currently taking place in the K-12 setting?

To our knowledge, this research represents the first comprehensive study of data and analysis to explore the nature of C3 educational awareness policies, initiatives, curriculum, and practices currently taking place in the U.S. public and private K-12 educational settings. It appears to be the first effort to establish baseline data for C3 awareness program design and provide the foundation for future studies on either expanding particular subject areas or examining progress. The National C3 Baseline Study was designed to provide a factual description of the state of C3 content being covered in U.S. K-12 settings. A literature review exploring current and pending Internet safety legislation and current research findings on online youth behavior, including social networking, chatting, and email, was conducted to provide context for the need for this survey. The literature review helped define further the study's major questions. The primary focus of the C3 Study was:

- 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 is the perceived importance of C3 content for U.S. K-12 school programs?
- What content is being delivered to educators, and how is it being taught?
- What, if any, are the issues and barriers that impede the delivery of C3 content in U.S. K-12 school programs?

Methodology

The National C3 Baseline Survey gathered and analyzed both qualitative and quantitative data from 1,569 public and private U.S. K-12 educators and ninety-four technology coordinators. This study used descriptive analysis relying extensively on a quantitative web-based survey (see Appendix D), designed specifically for the study, to assess the nature and extent of Cyberethics, Cybersafety, and Cybersecurity (C3) learning in U.S. K-12 schools, and to gather educators' perception of the importance of C3 content for both educators and students. The web-based survey was organized around the C3 framework with questions derived from the literature review. Input was added from educational organizations, Internet safety curriculum providers, security specialists, and C3 experts. Numerous edits and several revisions were made before a pilot was tested with a select sample of educators, technology coordinators, and state technology directors. Analysis and feedback gave rise to a final edition. The survey was split into two versions—one for classroom educators, and one for local education agency technology coordinators. Recruitment for the survey was done through email invitations distributed through multiple means including working with the State Educational Technology Directors Association (SETDA); State, regional, and local educational organizations; special interest groups; and educational media groups. ETPRO supplied the email invitation to send to participants. The invitation contained a brief description of the survey, a URL where the survey could be completed, and information for the respondents to use to activate their survey form. To encourage a larger response, we offered ten IPOD® Shuffle MP3 players to educators, awarded by a drawing. All potential participants were informed of the funding source (National Cyber Security Alliance), and who was conducting the survey (Educational Technology Policy, Research,

and Outreach) and were told that "All information you provide will be kept confidential**."** All data presented in this survey has been rendered anonymous; it is not possible to identify a particular respondent from the data. No data in this survey were out of range values. Missing data were investigated to determine cause and coded as either *not applicable to the respondent* (structural), or *applicable but no reply* (non-response). For the purpose of this baseline survey, we only used completed surveys or surveys with only structural missing data. Data were input into the SPSS 16.0 statistical package for analysis.

Qualitative Data

Some questions provided room for comments, or allowed the selection of *Other (Please specify)* coupled with a textbox for entry—for example, which Internet safety curriculum they used, and their preferred informal means of receiving information. We also collected qualitative data by means of educator, technology coordinator, and state technology director focus groups and individual interviews. A total of 219 educators, LEA technology coordinators/directors, and state technology directors and/or their representatives participated. Discussions were conducted with participants in an attempt to both verify survey results and gain further insights into findings reported through the survey. The interview participants were chosen to provide a wide-range of diversity. We selected educators by their various roles/positions (math teacher, music teacher, media specialist, technology resource teacher, elementary, middle and high school etc.), geographic location and demographics (state and school size), and number of years teaching. Each session lasted between one hour and one hour and twenty minutes. No comments in the survey include any individual identifying information. In some cases, minor grammatical or spelling errors were corrected, but no change was made to meaning. Appendix E includes the focus group/interview protocol.

The survey data were examined via a variety of statistical methods including means,[xxi] standard deviations,[xxii] confidence intervals,[xxiii] and other appropriate regression analysis among the variables. Tables and figures included in this report were chosen to best represent the data to the reader. They do not include all analysis completed, but do represent conclusions that are consistent with the rest of the analysis. It should be noted that in some cases, percentages in a table or figure may not add to 100% because of rounding. Additionally, in some cases, multiple selections were allowed, and percentages represent respondents who chose that answer; total percentages for these questions are not intended to add to 100% and may total to significantly higher percentages. Although all questions were intended to be as clear as possible, due to the delivery mechanism (an online survey), it is possible that differences in context may have resulted in different interpretations of the questions. The reader should therefore be conscious of this when interpreting the presented data. The census reported in 2004 that there were 6.2 million teachers in the United States.[xxiv] Given this population, and a confidence level of 99%, statistics indicate that the percentage of respondents who selected an answer should be within 4% of what would have been the result if the entire teacher population were surveyed. Additionally, it should be noted that the web-based survey was completed online and therefore assumes a minimum competency with the Internet. However, in 2004, the National Center for Educational Statistics (NCES) reported near universal access to the Internet in schools as of the fall of 2003,[xxv] and therefore the survey should have been universally accessible to educators.

Participant Demographics

The content portion of the C3 Baseline Survey was completed by 1,569 educators. In data collection, participants are sometimes reluctant to share personal information. As one respondent shared, "We are a small community and if you reveal information regarding job title along with location it may not be anonymous. Easy to tell who is who when there is only one _____ in your local area." Demographic questions were optional. However, approximately 85% of the respondents chose to answer these questions. Table 2-1 displays collected demographic information. Each category is then graphed in Figures 2-1 through 2-9.

Figure 2-1 shows the gender breakdown of the respondents of the survey. This compares well with the figures reported by the NEA[xxvii] that in 2006, males made up 24.4% of the U.S. public school teachers. We can conclude that the survey appears to have been completed by an appropriate cross-section of teachers by gender.

Figure 2-1: Gender

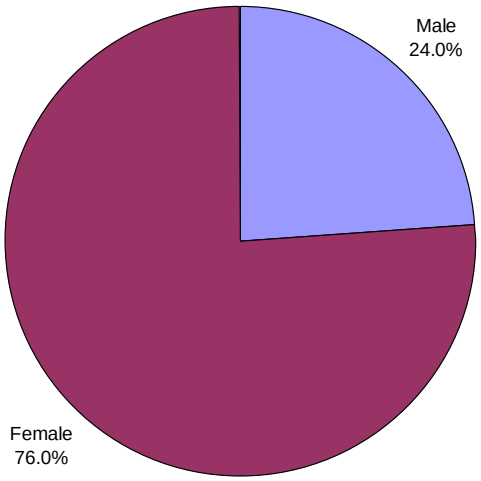


Table 2-1: Demographics

Subgroup	Number of Educators	Percentage of Total
Gender		
Male	374	24.0%
Female	1185	76.0%
Age		
18-24	24	1.5%
25-29	158	10.1%
30-34	159	10.1%
35-39	190	12.1%
40-44	176	11.2%
45-49	226	14.4%
50-54	287	18.3%
55-60	277	17.7%
Over 60	72	4.6%
Geographic region[xxvi]		
Northwest	367	26.8%
Southwest	265	19.4%
Northeast	432	31.6%
Southeast	305	22.3%
School Location		
Rural/Farming	314	22.8%
Small Town (2500-25,000)	347	25.2%
Large Town (>25,000)	140	10.2%
Mid-Size City (50,000-250,000)	173	12.5%
Suburb of Mid-Size City	110	8.0%
Large City (>250,000)	135	9.8%
Suburb of Large City	160	11.6%
School Type		
Public	1305	94.0%
Independent	12	0.9%
Charter	41	3.0%
Parochial	31	2.2%
Type of Certification		
Provisional	165	11.9%
Certified	1224	88.1%
Years of Teaching Experience		
First Year	23	1.7%
2-5 years	209	15.3%
6-10 years	269	19.7%
>10 years	866	63.4%
Grade Taught		
PK-5 (Elementary)	360	27.4%
6-8 (Middle)	267	20.3%
9-12 (High)	425	32.3%
Elem/Middle	116	8.8%
Elem/High	5	0.4%
Middle/High	83	6.3%
Elem/Middle/High	58	4.4%
Job Title (Multiple Selections Allowed		
Technology Specialist	174	
Classroom Teacher	1067	
Media Specialist	99	
Counselor	75	
Resource Teacher	54	

Figure 2-2 shows the age distribution of respondents to the survey. NCES breaks down educator groups into slightly different categories and states that in the U.S., 17% of teachers are under 30, 24% of teachers are 30-39, 25% are 40-49, 29% are 50-59, and 4% are 60 or over.[xxviii] Mapping our respondents to the same groups as NCES yields percentages of 11.6%, 22.2%, 25.6%, 35.9%, and 4.6%.

Figure 2-2: Age

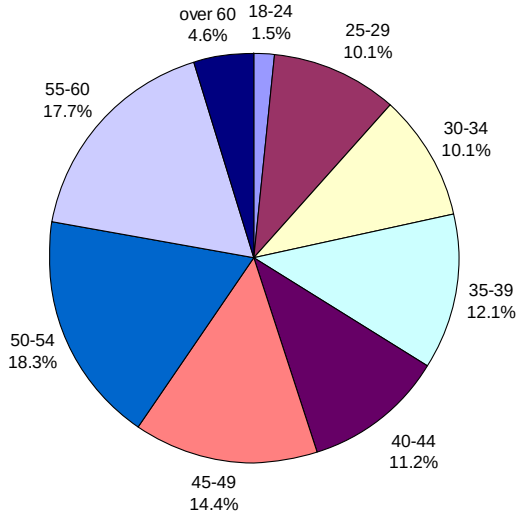
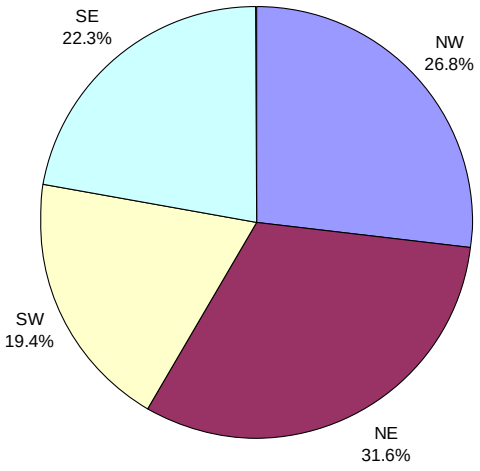


Figure 2-3 graphs educator locations. Respondents were distributed well across the country. It should be noted that responses were received from all fifty states.

Figure 2-3: Geographic Region



Respondents were also asked to describe the size of the community in which they lived. Their responses are shown in Figure 2-4; they represented a cross-section of communities in the US.

Figure 2-4: School Location

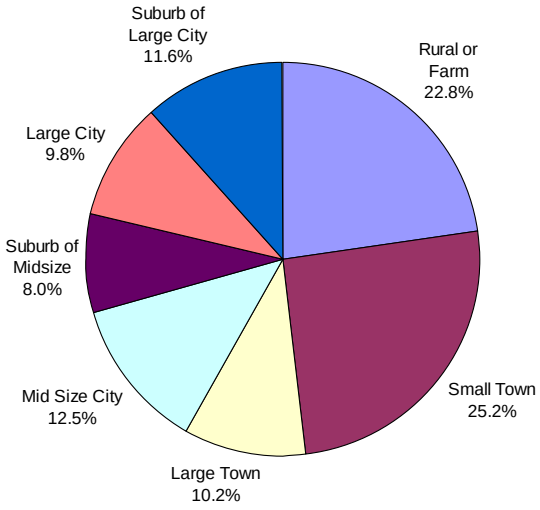
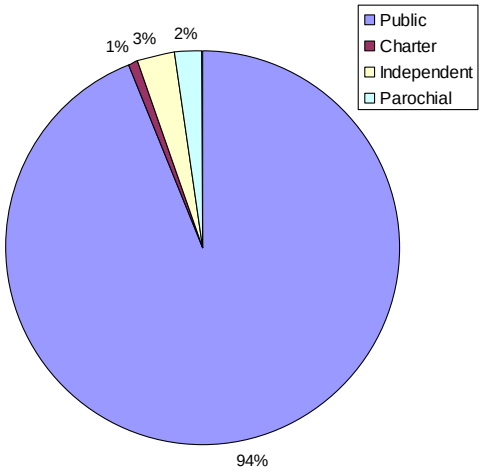


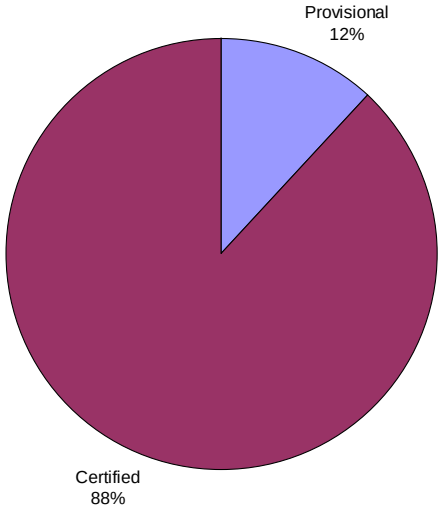
Figure 2-5 shows that the respondents to the survey were predominantly public school teachers (94%). The Center for Education Reform[xxix] lists this group as closer to 84% of all teachers. However, since we seek to influence public policy, understanding the problem in public schools will have maximum impact.

Figure 2-5: School Type



In Figure 2-6, the type of teaching certification for respondents is shown. The provisional certification category includes those who are receiving an alternative certification, those who have satisfied all requirements except a probationary period, those who require additional college coursework, and those who must still complete a certification program. NCES lists these groups as 10.4% of teachers.

Figure 2-6: Type of Certification



Comparing Figure 2-7, years of teaching experience to NCES statistics cannot be done exactly as they used a different breakout of ages. Combining two groups to create a ten-and-greater group for the NCES information yields a total percentage of 56.7% compared to 63% in our survey. NCES lists 27% in the four to nine years experience group, and 16.4% with less than three years experience. These numbers cannot be compared directly to this survey, but appear to be similar.

Figure 2-8 indicates the grades taught by the respondents. For the purpose of this survey, Elementary School was defined as PK-5, Middle School as grades 6-8, and High School as 9-12.

Figure 2-7: Years of Teaching Experience

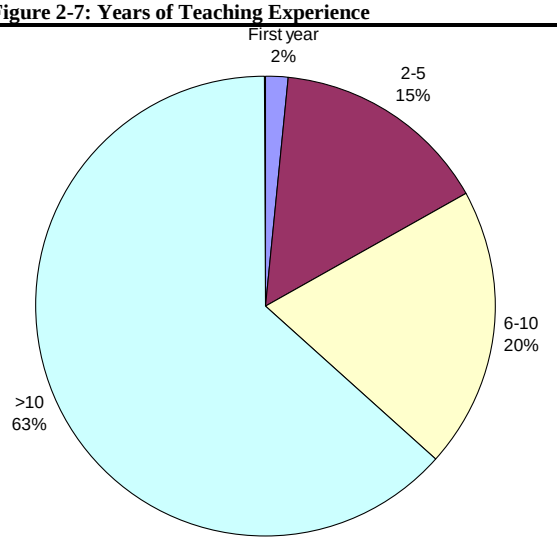


Figure 2-8: Grade Taught

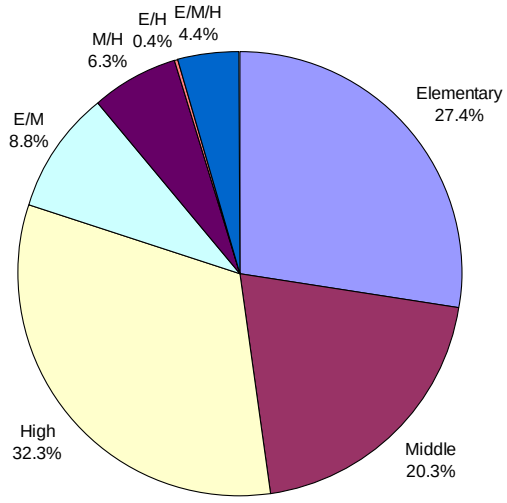
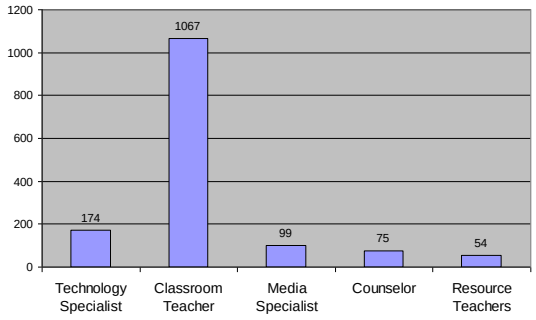


Figure 2-9 lists the job titles indicated by survey respondents. Particularly in the case of small schools, classroom teachers served as technology or media specialist in addition to their other duties.

Figure 2-9: Job Title (Some Have Multiple Jobs)



ENDNOTES

[xii] Center for Academic Integrity Study: Student Cheating in American High Schools. Donald L. McCabe May 2001 http://www.academicintegrity.org/

[xiii] The National Crime Prevention Council Stop Cyberbullying Before It Starts. Note that cyberbullies can be can be classmates, ex-friends, online acquaintances, and even anonymous uses http://www.ncpc.org/resources/enhancement-assets/ncpc_cms/cyberbullying-pdf

[xiv] See Pew Internet and American Life Project Reports: Family, Friends and Community. http://www.pewInternet.org/PPF/r/152/report_display.asp

[xv] Federal Trade Commission 2007 Identity Fraud Survey Report. Javelin Strategy and Research http://www.privacyrights.org/ar/idtheftsurveys.htm#Jav2007

[xvi] See McAfee-NCSA Online Safety Study full report at http://staysafeonline.org/pdf/McAfee_NCSA_analysis.pdf

[xvii] CSI 2007 Computer Crime and Security Survey. http://www.gocsi.com/

[xviii] SANS Top 20 2007 Security Risks. http://www.sans.org/top20/

[xix] SANS Top-20 2007 Security Risks: http://www.sans.org/top20/

[xx] For example, Kentucky has sent a bill to its legislature on February 13, 2008 (House Bill 367), and Virginia (HB58 – Approved March 7, 2006), passed a law requiring students to be taught about Internet Safety, and in Illinois, The Kotowski Internet Safety Bill (Public Act 095-0509 - http://www.ilga.gov/legislation/billstatus.asp?DocNum=1472&GAID=9&GA=95&DocTypeID=SB&LegID=29564&SessionID=51 states that each school may adapt an Internet safety curriculum and recommends 2 hours of Internet safety content per year; in New York Bill A08333 http://assembly.state.ny.us/leg/?bn=A08333&sh=t ; Texas SB 136 Internet Safety Curriculum and Texas HB3171 Internet Safety: makes available curriculum for use to schools http://www.capitol.state.tx.us/BillLookup/History.aspx?LegSess=80R&Bill=SB136 and http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=80R&Bill=HB3171

[xxi] Means in this context are arithmetic averages of the responses.

[xxii] Standard deviations are a measure of the variability of the responses. In this survey we use the formula $\sqrt{\sum\left(x-\bar{x}\right)^2 \Big/ \left(n-1\right)}$ where x is an individual sample, $\bar{x}$ is the mean of the population, and *n* is the number of respondents

[xxiii] Confidence intervals are computed at the 0.05 level. In other words, there is a 95% probability that the true population mean lies within the range defined by $\bar{x} \pm C$, where *C* is the confidence interval.

[xxiv] U.S. Census Bureau Special Edition for Teacher Appreciation Week – 2004 http://www.census.gov/Press-Release/www/releases/archives/facts_for_features_special_editions/001737.html

[xxv] NCES: Internet Access in U.S. Public Schools and Classrooms.

http://nces.ed.gov/surveys/frss/publications/2005015/index.asp?sectionID=2

[xxvi] *Northwest*: Alaska, Idaho, Iowa, Kansas, Minnesota, Missouri , Montana, North Dakota, Nebraska, Oregon, South Dakota, Washington, Wyoming, *Southwest*: Arkansas, Arizona, Colorado, California, Hawaii, Louisiana, New Mexico, Nevada, Oklahoma, Texas, Utah, *Northeast*: Connecticut, Delaware, District of Columbia, Illinois, Indiana, , Massachusetts, Maryland, Maine, Michigan, , New Hampshire, New Jersey, New York, Ohio, Pennsylvania, Rhode Island, Vermont, Wisconsin, *Southeast*: Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee Virginia, , West Virginia – Extracted from http://memory.loc.gov/ammem/gmdhtml/rrhtml/regions2.html

[xxvii] Rankings & Estimates. Rankings of the States 2006 and Estimates of School Statistics 2007. NEA Research. December 2007. Available at: http://www.nea.org/edstats/images/07rankings.pdf

[xxviii] Contexts of Elementary and Secondary Education. Available at: http://nces.ed.gov/programs/coe/2007/section4/indicator33.asp#info

[xxix] K-12 Facts. Available at http://www.edreform.com/index.cfm?fuseAction=section&pSectionID=15&cSectionID=97

3

How does the Educational System Inform Students about C3 Topics?

I feel that these issues are viewed as "not important" by the district. They are more focused on teaching standard curriculums that pertain to state test scores. Cyber "anything" is viewed as non-relevant or not the district's responsibility to teach. (Northwest LEA Technology Coordinator/Director)

Most of the issues you have mentioned during this survey receive very little attention, if any, by administrators or the State. For all the years I have been associated with IT_15 yrs_I have read of the need to educate people on safety and security issues. However, the need is rarely recognized outside of the IT world. (Northeast LEA Technology Coordinator)

It seems to me that our district places a lot of emphasis on protecting users from inappropriate sites by blocking on a widespread basis. There is little or no curriculum dealing with teaching HOW to use technology appropriately. (Southeast Educator)

By and large our district does little or no cyber education. (Southwest Educator)

To the best of my knowledge we have NO program in place to educate adults or students in regards to cyber anything. (Southwest Educator)

Interesting to see how little we cover these issues in our district (Southwest LEA Technology Coordinator/Director)

The primary purpose of the National C3 Baseline Survey is to better understand how Cyberethics, Cybersafety, and Cybersecurity (C3) awareness, curriculum, and practices are currently being addressed in the U.S. public and private K-12 educational settings. With the recent increase in media coverage describing issues related to cyberbullying, online predators, identity theft, social networking, spam and malware, we were interested in examining if and how schools are prepared to address these topics. The statements above are just a handful of the comments shared by survey participants who indicate surprisingly limited curriculum, instruction, or presentation taking place in today's K-12 setting. Respondents indicated that local education agencies outline some C3 limitations on IT use in their Acceptable Use Policies (AUP) and student handbooks. However, these restrictions are often driven by legal issues and protections for the school rather than a focus on informing and providing safety for the individual. What appears to be missing is information regarding reasons behind these restrictions and a much-needed focus on instructional aspects of C3. Furthermore, educators revealed that standards documents may include technology topics, but

- Over half of educators' responses revealed they do not know how their school informs students about protecting against, identifying, and responding to cyber-crime (e.g. identity theft, predators, cyberbullying, etc).
- Almost 60% of educators surveyed indicated they do not know how their school informs students how to identify signs that documents and emails may contain viruses.
- 34% percent of educators stated that technology standards either do not or only peripherally address Cybersecurity.
- Almost 30% of respondents indicated technology standards either do not or only peripherally address Cybersafety or Cyberethics.
- Policies focus on restrictions. Curriculum may include technology skills but only has limited content on C3 topics.

they are couched in general statements and tend to focus on technology skills, not C3 topics. Rather than providing guidance on specific areas, these standards offer broad statements without interpretation. This has resulted in a narrow view of "Internet safety," focusing primarily on online predators, precautions on social networking sites, and "stranger danger" campaigns. Educator respondents indicated that C3 topics were rarely presented in one day assemblies, state curriculum, or health/safety curriculum: less than 9.1%, 8.6%, and 12.7% respectively. Educators believe that outside presentations have, at best, made limited impact on students. As perceived by survey respondents, primary responsibility for conveying C3 content to students rests with educators.

This data should not be used to downplay programs such as the Safe Schools/D.A.R.E. initiatives, numerous state-wide attorney general Internet safety campaigns, national Internet safety programs (i.e.,Netsmartz, iSAFE, WebWiseKids, iKeepSafe, CyberSmart!), or assembly efforts and training for students, parents and educators. However, even the closest thing to curriculum embedded through the Safe Schools initiatives allow for only one or two lessons plans which focus on specific topics. This limited exposure time could be a cause of educators feeling they have provided only minimal impact on students, addressing a narrow set of safety topics.

Cyberethics

To better understand how students are made aware of Cyberethics, Cybersafety, and Cybersecurity (C3) content, one of the first questions asked of educators and local education agencies (LEA) tech coordinators was: *How does your school/school district inform your students about specific laws, policies, and guidelines related to the ethical use of resources?* The results are shown in Table 3-1.

At first glance, some of the data look rather promising. For example, copyright policies and procedures are included in student handbooks (59.7%) and Acceptable Use Policies (63.5%), AUP and student handbooks are sent home for review (67.3%), and both are reviewed at the beginning of the year (59.2%). Respondents indicate extensive modeling and encouragement of appropriate ethical behavior (72.6%). This claim may be contradicted in other parts of the survey, depending upon in-

Table 3-1: [Educator Survey] How school/school districts inform students about ethical use of resources

N=1569	Yes Percentage
presentation of copyright information at the beginning of the term in an orientation class	25.2%
presentation of copyright information at the beginning of the term in my class	32.7%
presentation of copyright information at the beginning of the year at an assembly	10.3%
presentation of copyright information at the beginning of the year by the media specialist	35.9%
modeling and encouragement of appropriate ethical behavior	72.6%
copyright policies and procedures included in student handbooks	59.7%
copyright policies and procedures included in Acceptable Use Policies (AUP)	63.5%
Acceptable Use Policies (AUP) and student handbooks sent home for review and/or signed by students and parents	67.3%
Acceptable Use Policies (AUP) and student handbooks reviewed at beginning of year	59.2%
Acceptable Use Policies (AUP) and student handbooks reviewed several times throughout the year	18.1%
provision of examples of bibliographic citations included in Acceptable Use Policies (AUP)	19.7%
provision of examples of bibliographic citations included in student handbook	15.9%
Dangers, consequences, and legal issues of downloading, filesharing, copyright violations in either the AUP or student handbook	31.9%

terpretation and is a focus of Section 4 of the C3 Baseline Study. Data reveal that, other than a handout or review at the beginning of the year, there is a lack of more extensive interaction with students on these topics. Only 18.1% indicate reviewing the policies throughout the school year. Only 19.7% of the respondents suggest that examples of the right way to cite references are provided in the AUP, and only 15.9% in the student handbook.

Thus, educators report that informing students about *policies* on copyright, downloading, and file sharing is covered by an AUP or student handbook, or a discussion in the beginning of the year, with limited follow-up. Only 31.9% of the respondents indicated the occurrence of sharing the *dangers, consequences, and legal issues* of downloading, file sharing, and copyright violations in either the AUP or student handbook. Follow-up interviews with educators helped illuminate the low response rate for this area. One educator shared, "I think they [student handbooks and AUP] mention not to do it…not tolerated, but there is no explanation as to why and definitely no consequences listed." Another typical response was, "I don't think there are consequences beyond what a teacher might do." The web-based survey allowed participants to enter comments related to how schools convey ethical topics to students. Table 3-2 shares some comments that were provided by educators.

The C3 Baseline Survey also tried to delve deeper into how educators perceived students being informed by their school or school system about Cyberethics, safety, and security areas related to specific topics. In spite of the data in Table 3-1 indicating that AUPs and student handbooks were used to inform students about policies, in Table 3-3, the data reveal that for many topics, either educators or

Table 3-2: Educator Comments: How school/school districts inform students about ethical use of resources

Generally English & study skills classes teach plagiarism and copyright	Recurring warnings in class	District wide presentation
When appropriate to the lesson	During research unit	On webpage
Discuss the topic, but not a full presentation.	In individual classrooms	N/A at elementary grade level
Within first semester	Teachers are expected to cover this information in English, Social Studies or Science class.	Some teachers do, most don't
During a specific unit of study	Copyright at registration	The librarian reviews this with each class
Upon teacher request	Handbook sent home in fall	These may be done at the middle and high school level, not the elementary.
Don't teach	Teacher initiated	Sporadic lessons attached to research projects

Table 3-3: [Educator Survey] Conveying Information

How does your school/school district inform your students about specific laws, policies and guidelines related to … (Check all that apply)

	AUP	Student Handbook	One Day Assembly	State Curriculum	Health/Safety Curriculum	Media Specialist	Educator	Not Sure	Other
How students can protect themselves from online cyberpredators	21.0%	24.6%	9.1%	6.8%	12.7%	31.5%	33.8%	38.9%	7.4%
Protecting, Identifying and responding to cyber-crime (i.e, identity theft, predators, cyberbullying, etc.)	12.9%	15.5%	6.8%	4.4%	8.2%	20.1%	26.2%	50.9%	5.2%
Consequences of plagiarism	23.3%	48.4%	3.9%	6.6%	2.7%	35.2%	57.3%	19.5%	2.7%
Correct citation and references	20.1%	14.9%	2.1%	8.6%	1.9%	39.4%	62.2%	22.6%	2.5%
How students can protect themselves on social networking sites and while chatting	5.9%	7.0%	6.8%	2.8%	8.5%	17.0%	26.3%	52.8%	5.3%
What students should do if they receive unsolicited emails or instant messages (information asking them to check out a picture, video or document, asking them to update account information or informing them they have won a prize)	4.8%	6.1%	4.1%	2.6%	5.7%	17.5%	25.7%	56.3%	4.6%
Legal, safe and appropriate practices for downloading files	20.0%	8.0%	2.4%	2.6%	2.8%	28.5%	29.7%	48.9%	3.3%
Characteristics of spam, avoiding its impact and spam filters	4.8%	3.6%	2.0%	2.1%	1.9%	18.7%	17.1%	0.0%	4.4%
Installing and updating firewalls, anti-virus, anti-spyware, and anti-spam software on computer	4.0%	2.7%	0.8%	2.3%	1.6%	22.4%	11.2%	56.5%	8.2%
How to make sure a website is transmitting information securely	2.8%	1.5%	0.8%	2.0%	1.3%	19.6%	14.0%	60.7%	5.0%
Signs of documents and emails containing viruses	4.0%	2.0%	0.7%	1.7%	1.1%	20.7%	13.1%	59.5%	6.6%
How to automate data backups	2.2%	1.1%	1.0%	1.1%	0.7%	19.9%	11.8%	61.2%	6.2%
How to patch an operating system, update browser(s) to the latest version, and/or patch productivity software (i.e., email program, office programs)	2.2%	1.0%	0.7%	0.9%	0.7%	18.5%	10.1%	62.1%	7.3%

media specialists were the primary means to provide information to the students. In most cases, more than half the educators were not sure how many of the topics were addressed.

Educators surveyed perceive the task of teaching Cyberethics related to plagiarism (consequences of plagiarism and correct citation and referencing*)* as primarily the responsibility of the individual educator (consequences 57.3%, correct citation 62.2%), followed by the student handbook (consequences 48.4%, correct citation, 14.9%), and the media specialist (consequences 35.2%, correct citation 39.4%).

Interestingly, very low numbers of educators felt that neither topic was addressed in the state curriculum (6.6% and 8.6%). Further comments shared by participants added additional insight. While educators perceive school systems placing the responsibility of conveying this information in the hands of the teacher, several focus group participants agreed with survey participants who wrote, "Plagiarism and how to cite is taught through media, English classes, and anyone doing research projects." Another participant shared, "Seniors only…in English I think." Teachers repeatedly stated that "most of this [citation process] is handled by the media specialist or English teacher." Several comments indicated that these topics were left to the individual teacher, and in most cases were rarely addressed, or educators directed students with simple statements such as "no cheating" or you "need to cite your sources." Some educa-

tors stated that discussions of plagiarism and proper citation were not relevant for their class: "N/A I teach math," and "it's just something extra…not really covered in my [content] area." They also indicated that they lacked the time needed to ensure compliance: "I just have no time to check all the papers." Finally, and perhaps key, they perceived that the school district did not view the issue as important: "I just don't think they are [plagiarism and copyright] viewed as very important [by school and school district]." Another educator stated, "It's easy to tell students they need to cite their resources, but I'm not sure I would really know the correct way to do it. I'd need to go back and brush up." Many who taught kindergarten or elementary listed in their comments, "N/A for my grade level," and "I teach in an elementary school. I don't think this is even addressed."

Even in cases where plagiarism is discussed, consequences are uneven at best. Describing consequences and the process, educators shared,

> *no real consequences for students if you do turn them in*
>
> *…usually have to handle it yourself. If you do something the parents complain*
>
> *cutting and pasting has just become so easy*
>
> *I reported a case to the administrator but because it would effect the student's playing* [a sport] *nothing happened*
>
> *…it* [reporting an incidence] *was a nightmare…parents came in and legal threats… it just wasn't worth it*

A few indicated, through interviews and by adding comments in the web-based survey, that policies regarding plagiarism, copyright, and cheating were also covered in their schools' honor code. However, even educators whose school had an honor code indicated that the primary responsibility for conveying information to students about ethical issues is left to the individual educator. In addition, many felt that trying to enforce consequences for plagiarism wasn't worth the trouble. One educator summarizes the common sentiment:

> *If it's not tested I don't worry about it. I focus on what the students will be tested on. That's what matters most to the state.*

Cybersafety and Cybersecurity

Even within student handbooks and AUPs, many topics in Table 3-3 are not well represented. Cybersecurity and Cybersafety issues are particularly troubling. These topics often were not addressed in the AUP or student handbooks (most topics ranged from 1.0% to 10.0%), and were addressed at a significantly lower percentage than Cyberethics by both educators and media specialists. In fact, the predominant answer by the respondents on *how schools/school districts conveyed information to students* was they were not sure how the school/district informed students about cybercrime (50.9%); protection on social networking sites (52.8%); responses to unsolicited online contacts (56.3%); legal, safe, and appropriate practices for downloading files (48.9%); installing and updating firewalls, anti-virus, anti-spyware, and anti-spam software (56.5%); how to make sure a website is secure (60.7%); signs of infected documents and emails (59.5%); how to back-up data (61.2%); or how to patch or update operating systems and software (62.1%). One-day assemblies and "other" were two additional options noted for each of these categories, although a small percent was indicated for each.

For the question, *How does your school/school district inform your students about specific laws, policies and guidelines related to … (Check all that apply)*, data were: protection from predators (one-day assembly 9.1%, other 7.4%); cybercrime (one-day assembly 6.8%, other 5.2%); protection on social networking sites (one-day assembly 6.8%, other 5.3%); responses to unsolicited online contacts (one-day assembly 4.1%, other 4.6%); legal, safe, and appropriate practices for downloading files (one-day assembly 2.4%, other 3.3%); spam and spam filters (one-day assembly 2.0 %, other 4.4%); installing and updating firewalls, anti-virus, anti-spyware, and anti-spam software (one-day assembly 0.8 %, other 8.2%); how to make sure a website is secure (one-day assembly 0.8%, other 5.0%); signs of infected documents and emails (one-day assembly 0.7%, other 6.6%); how to backup data (one-day assembly 1.0%, other 6.2%); or how to patch or update operating systems and software (one-day assembly 0.7%, other 7.3%). Those who chose "other" indicated a variety of presentation modes. Cybersafety material was presented to students through: building-based support teams; computer classes (if the student chose this as an elective); school security officers; School Resource Officer (SRO) class; school counselors and resource officers; bullying-prevention initiatives; Safe School initiatives; Future Business Leaders of America (FBLA) presentations; counselors; and technology coordinators and specialists. Outside presentation sources included Internet safety awareness curriculum organizations, state attorney general initiatives, Drug Abuse Resistance Education (DARE) officers, community agencies, and police guest speakers. Additionally, these outside agencies presented to parent groups and parent teacher associations (PTA). A few indicated "ethics" training for students enrolled in virtual high school courses. While there certainly were many examples of efforts underway, participants indicated that presentations were usually stand-alone, often one-time assemblies or presentations which were narrowly focused. Topics listed as being addressed specifically dealt with Internet predators, cyberbullying, and precautions when using social network sites. Content presentations regarding plagiarism and resource citation were introduced to students through a freshman class, English/Literature Arts classes, and an 8th grade three-week computer class. Additionally, information was provided through handouts and on school and county websites. It should be noted that the option of "other" quantifies a small percentage, and presentations were reported as usually occurring once a year, at best. Those who choose "other" for all topics related to security (downloading, spam, firewalls, anti-virus protection, secure websites, viruses, backups, and patches) indicated that the schools/school districts conveyed information to students on these topics by eliminating opportunities (e.g. downloading was not allowed, students could only go to pre-selected and filtered websites, and/or no email access was allowed). While the perception was that schools were covering the topic, the mechanism did not promote awareness of the topic; they simply eliminated access. This is an area of debate. Filtering is mandated to receive E-rate funds by the Children's Internet Protection Act,[xxx] but civil liberty groups, teachers, and students complain that the software is ineffective and blocks access to many sites relevant to educational resources. The Deleting Online Predators Act[xxxi] has been proposed to expand filtering to social networks and some schools are already implementing its guidelines. Just like new drivers take a driver education class, and all must pass a basic test to show they understand the laws and a driving test to indicate they can drive, one would assume students would be given some instruction, and measured on basic ethics, safety, and security competencies to use ubiquitous communication and research tools. Monitoring tools, like driver education, are

finite. At some point students will have to leave the parking lot and be out on the highway without the district's IT infrastructure. Whether students will be ethical, safe, and secure without someone watching over them is a question the educational community might need to consider.

In terms of Cybersecurity and Cybersafety, participants shared these comments:

> *Cybersecurity issues are largely dealt with through our office of technology. Downloads are blocked and updates are done centrally. All secondary students have logons and passwords.*

> *My students are very low functioning and so I do not personally go in depth with them, however we do have very good_too good_firewall and we monitor all computers our students use in the classroom.*

> *The students rarely use the web to do research or any other type of activity than the controlled, pre-selected programs. There is a strong filter that denies access to any blog site and most controversial sites.*

> *We do not allow the use of any social networking sites on district technology.*

> *Filters disable chats.*

> *Blogs are not now being used at this school; there is no social networking at the school site other than teachers emailing to one another; no instant messaging capabilities at this school.*

While there were some positive comments about the effectiveness of the IT departments, negative comments were far more frequent.

> *Students and myself are very dissatisfied by the excessive firewalls at school.*

> *We do a pretty good job protecting students when they are on our own network within the school and address issues regularly dealing with acceptable use. We don't do well teaching them how to function safely and ethically OUTSIDE of the school environment. Partially that's because it's not a state standard that we are required to teach, and, while we all care about students, there's only so much time in a day to teach what we HAVE to teach.*

> *We teach cyberethics and safety in the library but not all classes participate. This is a problem.*

> *A lot of these issues aren't addressed at the elementary level, especially kindergarten*

> *My school district does not really educate students on how to avoid all these Internet pitfalls, but rather, has a very thorough blocking practice which just doesn't let anyone get on anything, pretty much.*

> *We "Addressed" it* [Cybersafety] *to parents at one meeting two years ago.*

Where safety lessons have been implemented, the primary focus has been on online predators and shielding students from "dangerous" issues (with firewalls and filtering), rather than informing them about the issues. In the words of one educator,

> *A lot of our cybersecurity and safety instruction is fundamentally flawed—focusing on the rare cases of adults pretending to be children and then forcibly abducting them. This does not reflect reality and doesn't serve our students well. Also, the things we don't let them do in*

school (social networking, email, media downloads, etc.) are things that many of them are not learning to use wisely.

There were two general camps regarding the coverage of safety and security topics. One camp feels that safety, and particularly security, should not be the responsibility of the teacher. This group feels that the responsibility lies with parents since most activity happens outside of class time. Educators also feel security doesn't apply since the school system locks down computers and therefore security awareness is not necessary. Concern also arises that teachers will be asked to cover yet another area of content in an already packed curriculum.

Although I answered that I do not have a lot of knowledge about CyberSafety and CyberSecurity, my district is very responsible about computer security and many things are in place at that level that I am not necessarily aware of. I feel that on the elementary level, it is important for my students to learn about cyberethics some security, but they do not need information [on] *firewalls, etc. at this point in their education.*

Time is of the essence...teachers are exhausted after a week of teaching and need a life - please keep the information to the point and not expect hours of reading etc. We have many extra hours, outside of the school day, on lesson plans, preparation and grading to do too!

I don't mind teaching about the dangers and benefits of the Internet, but I will resent it if teachers are, once again, expected to do a parent's job. Ultimately, it is the parent's job to set limits and explain what is and is not acceptable when using the home computer, as well as monitoring their children's access.

Much of what you survey here has nothing to do with teachers. It is the sole responsibility of students and parents.

Most of what you asked about does not really apply to classroom teachers except for plagiarism issues. Leave the security to the tech support people and let them tell us what we need to know!

We are a kindergarten through fourth grade school. Many of these issues do not apply to our circumstances.

A lot of the survey questions don't apply much/at all to me as I teach 9 and 10 year olds. At this age, we teachers have to be specific about the site we want students to go to for information.

So, some educators have reached the conclusion that by "securing" the computer domains at school, Cybersecurity and Cybersafety are not a concern, and they have limited, if any, responsibility to address it.

The other camp, as indicated through both the web-based survey and focus groups, believes there is a need to cover Cybersafety and Cybersecurity in schools. They are also interested in knowing more on the topics for their own edification. Some noted an increasing number of issues arising inside and outside of class time, that carry over and impact classroom instruction.

Recently, our school district (the high school that our middle school feeds to) had a student break into the system and change student grades. It made big headlines! I would love to know more about protecting myself from hacking, and would love to be able to better educate my students about all of the factors involved in C3. I definitely think this is a worthwhile

cause that needs to be addressed regularly and in-depth with students of all ages.

A common concern expressed by participants in the qualitative interviews revolved around cyberbullying. Several participants also shared similar concerns through the web-based survey.

We have a large population of girls being mean to girls on the Internet and then carrying it to school.

We have had incidents this year of videos featuring bully behaviors directed toward a student posted on YouTube by other students in our school. This has been very eye-opening about the lack of supervision students have when away from school.

As a counselor I am privy to the horrendous bullying/harassment and poor judgment by children and young adults on the Internet and cell phones. I would like to see a comprehensive K-12 plan addressing the C3 instruction in all schools. I would be willing to help promote this in my school and beyond.

Although some educators did not see an immediate need for Cybersafety and Cybersecurity education in their elementary schools, they recognized the ever-growing dependency on the Internet and recognized the need for future training would be needed.

Due to the restrictions that the school district places on student accounts, it is really difficult to teach them about spyware blockers & detection or virus software or firewalls. Students do not have access to desktops, many of our low income students use public access computers so it is vital for them to understand security issues. Media literacy and safety needs to be required - like we used to teach keyboarding. Our teachers need to know more. We are developing lessons to incorporate this into content courses - but it needs to be required and monitored to ensure it is done. The hours I listed as our division/school providing staff development in Internet safety are hours I have spent training our staff but I am one out of 5 high schools and this is not happening at the other 4 high schools.

I feel that many of these issues don't pertain to our school--the kids don't have cell phones (yet!) and many homes don't even have Internet yet. However, I can see the time coming when I will have to address all these issues.

These findings suggest that educators recognize that students are receiving limited instruction on Cybersafety and Cybersecurity. Teachers are concerned that the time commitment for this additional subject matter would negatively impact their ability to meet the demands of other curriculum. Even so, they are aware of the importance of this topic to students in both their educational environment and in their home usage. Media coverage and local instances of inappropriate student behavior reinforced educators' awareness of the need for C3 training for themselves and their students.

Local Education Agency Technology Coordinators

With the growth of the Internet, several local education agencies (school districts) have established a full-time technology coordinator position. This person not only keeps track of relevant technology, but also, more importantly, is expected to identify, design, conduct, and maintain technology professional development for educators, attend technology meetings, help with grants and funding, and inform and assist in the introduction of technology-

integrated curriculum. As part of the C3 Study effort, a separate survey was created to extract their perspectives.

When technology coordinators were asked *Does your county/district/school system use an external Internet safety curriculum (i.e., CyberSmart!, iKeepSafe, i-SAFE, NetSmartz, etc.),* 39% indicated yes, but 61% answered no. Additionally, many did not specify a curriculum. They cited web filtering and protection mechanisms used to protect the systems, rather than instructional content for students. In web-based comments and follow-up interviews, respondents indicated that, in cases where an outside Internet safety curriculum was used, "we've had assemblies, but not adopted a curriculum." "One-class police presentation," "DARE officer does a safety presentation with some classes," and "school cop, security officer, human relations class" were the primary resources. Furthermore, coordinators shared "the majority of presentations have focused on Cybersafety." Most of the presentations have been about "predators…not to give out information, not to trust anyone on the Internet." A limited number of technology teachers who had integrated content into the classroom confirmed the coordinators' responses.

> *Although our district does not have a program for teaching Internet safety, I have used a Netsmartz lesson with my students…safety issues.*

Again, the focus was on Cybersafety, and Cybersecurity was not recognized as a separate issue. However, even for some teachers trained to teach Cybersafety, the opportunity to deliver the content was limited.

> *I work in a K-5 school. I service approx. 700 students a week for 30 min. As far as I am aware, there is not much done w/technology or its issues aside from class time with me. I am iSAFE certified, but have not been given permission to use it in my district at this time.*

> *In my technology class, I have done one Netsmartz lesson with each class on Cybersafety—geared for the appropriate grade level.*

Technology coordinators were asked how the group they supported (county/district/school) presented C3 to students (See Table 3-4). Questions ranged from promoting proper and responsible computer use through model lessons, to providing document examples and including each C3 topic within the classroom. A response of 1 indicated *Not at All*, and 5 indicated *a great deal.* As previous information in this section indicates, C3 topics were rarely required to be taught in the classroom—Cyberethics had a mean of 2.14, Cybersafety, 2.01, and Cybersecurity 1.94, indicating an average value one step away from no instruction at all. C3 topics were not required by the curriculum guides (mean of 2.19). Most surprisingly, C3 awareness was only marginally included within model lessons. In practice, technology coordinators often are more closely tied to technology goals within the local education agency (LEA), and these results most likely represent a best case of what is intended. Actual inclusion of C3 instruction may be even lower.

As Table 3-5 indicates, LEAs are moving forward with written policies describing appropriate use of computers and the Internet for both students and educators. Students almost universally are required to agree to such a policy (96.5%), and educators at 89.5%. However, this may not be driven by an educational imperative. Instead, this may be driven by the legal community and LEAs may be looking to protect themselves from legal repercussions of improper IT use.

This concern for legal repercussions can be seen in Table 3-6, which describes the measures, both informational and technological, LEAs take to protect their networks from both

Table 3-4: [Coordinator Survey] How is C3 presented to students

How is your county/district/school promoting various types of student awareness of Cyberethics, Cybersafety and Cybersecurity? To what extent does the county/district/school use the following strategies/policies? Rate 1-5 scale (1 not at all – 5 a great deal) My county/district/school promotes student proper and responsible use of computers by…		
	Mean	±*
Including cyberethics awareness in the curriculum (as "good practice" or in model lessons given to students)	2.80	0.269
Including cybersafety awareness in the curriculum (as "good practice" or in model lessons given to students)	2.69	0.258
Including cybersecurity awareness in the curriculum (as "good practice" or in model lessons given to .students)	2.64	0.270
Ensuring that cyberethics, safety and security topics are included in documents as a good example of integration technology in the curriculum	2.37	0.247
Implementing a policy that requires cyberethics, safety and security be required in the county/district/school curriculum	2.19	0.283
Requiring cyberethics be taught in the classroom setting	2.14	0.267
Requiring cybersafety be taught in the classroom setting	2.01	0.260
Requiring cybersecurity be taught in the classroom setting	1.94	0.236

Table 3-5: [Coordinator Survey] Written Policies

Does your county/district/school have written policies regarding the appropriate use of computers and the Internet by students and/or educators? Our county/district/school has written policies regarding appropriate use of computers and the Internet for:		
	Yes	No
Educators	89.5%	10.5%
Students	96.5%	3.5%

hackers and inappropriate contact. Of the technology coordinators surveyed, 93.2% indicated their LEA filtered Internet content, 88.5% block Internet content, and 87.5% of teachers/librarians/media specialists monitor Internet use. Although 96.5% of LEAs have written policies for the students, technology coordinators indicated 80.7% of students must sign a contract agreeing to the policy. These contracts are often more tied to individual school rules (computer lab rules), whereas an AUP is written by the school board for an entire district. However, in spite of this high percentage of schools that impose written restrictions on computer use, the AUP is only updated yearly in 63.6% of schools, and professional development on appropriate use is only provided in 61.4% of cases. Thus, many schools have focused on one-time policy construction and/or hardware protection, and not the instructional side of Cybersafety and Cybersecurity.

When asked about laws, policies, and guidelines regarding ethical uses of resources, a large number of coordinators indicated this

information was included within student and staff handbooks (73.9%), and modeling and encouragement of appropriate behavior was prevalent (64.8%). Although these percentages are higher than many earlier categories

Table 3-6: [Coordinator Survey] Policies and Procedures

What types of policies and/or procedures does your county/district/school use to ensure appropriate use of technology and the Internet? (Yes, No, Not Sure, Other-text)				
	Yes	No	Not Sure	Other
Students must sign a "contract" agreeing to use computers for appropriate purposes	80.7%	14.8%	2.3%	2.3%
Teachers and librarians/media specialists use classroom management techniques to monitor use and instruct students on appropriate use	87.5%	5.7%	5.7%	1.1%
Teachers and librarians/media specialists receive professional development on the appropriate use of the Internet in their classrooms	61.4%	28.4%	8.0%	2.3%
Filters (i.e., a mechanism to limit Internet access to certain forms of information) are installed on computers	93.2%	3.4%	2.3%	1.1%
Social networking sites are blocked	88.5%	6.9%	2.3%	2.3%
The Technology Acceptable Use Policy Is updated each year	63.6%	29.5%	4.5%	2.3%

Table 3-7: [Coordinator Survey] Ethical Use Policies

How does your school/school district inform your students and teachers about specific laws, policies and guidelines related to the ethical use of resources?	
	Yes Percentage
copyright notices on appropriate equipment throughout the building	36.4%
modeling and encouragement of appropriate ethical behavior among staff and students	64.8%
copyright policies and procedures included in student and staff handbooks	47.7%
AUP policies and procedures (that address ethical use of material) included in student and staff handbooks	73.9%
provision of examples of bibliographic citations	48.3%
up-to-date file of copyright permissions, purchase orders, software licenses or documentation, etc., to document legal compliance.	45.5%

one may still question why these topics are not included and covered universally. Integrity and ethics as a cornerstone of behavior is only being included in seven out of ten LEAs. Additionally, over half the LEAs (see Table 3-7 for more detailed breakdown), did not provide examples of proper citation or include proper copyright notices when needed.

Interestingly, Table 3-7 and Table 3-1 indicate a disconnect between the opinions of the technology coordinators and educators. For example, in Table 3-1, educators indicate that they believe students are informed about ethical use of resources by modeling and encouragement of ethical behavior at a rate of 72.6%, although in Table 3-7, coordinators indicate this occurs in 64.8% of cases. Similarly, when asked if copyright policy is included in student and staff handbooks, 59.7% of teachers say yes, whereas coordinators believe this occurs in 47.7% of the time. Clearly there is a discrepancy between what coordinators and teachers perceive is happening in the school setting, and what each believes is included in ethics policy. Perhaps this is a difference in perspective. Coordinators may misunderstand what is going on in the classroom, and both groups

may have a different understanding as to what the policies are trying to describe. This discrepancy should be investigated further.

The C3 Survey also asked technology coordinators to identify whether technology-use policies (AUP, student code of conduct, or other documents) address specific areas. The results are shown in Table 3-8. The topics cover explanations and consequences of digital plagiarism, strong passwords, cyberbullying, social networking guidelines, cell phone use, and other areas of interest. Some categories are improving: plagiarism explanations are included in 62.2% of cases, cyberbullying in 59.6% of schools, cell phone use is addressed in 74.4% of schools, monitoring of social networking sites in 59.1%. However, there are still major topic areas that do not appear to be addressed (*Not covered* or *Not Sure* categories): 73.9% of schools do not explain strong passwords, 70.2% do not outline early signs of virus and phishing attacks, and 69.9% do not explain protection from phishing attacks. Clearly AUPs and student handbooks need to be expanded to cover these key current topics, as technology best practices list these areas as a minimum set to ensure students and educators understand proper use and protection of the LEA IT infrastructure.

Table 3-8: [Coordinator Survey] Technology Use Policy

	AUP	Student Code of Conduct	Not Covered	Not Sure	Covered in Other -Specify
Explains digital plagiarism (cutting and pasting) and lists consequences	42.6%	17.0%	26.6%	10.6%	3.2%
Explains to students and educators how to set up a strong password	19.6%	0.0%	67.4%	6.5%	6.5%
Addresses cyberbullying	39.4%	19.1%	34.0%	6.4%	1.1%
Social networking guidelines and expectations are detailed	40.9%	6.5%	40.9%	8.6%	3.2%
Cell phone use addressed	20.4%	51.6%	20.4%	5.4%	2.2%
Requires monitoring of students' social networking sites (related to classwork)	40.9%	6.5%	35.5%	5.4%	11.8%
Addresses accessing local school system wireless account from personal computer	42.7%	5.6%	43.8%	2.2%	5.6%
Addresses accessing local school system wireless account from PDA or cell phone	30.3%	5.6%	57.3%	4.5%	2.2%
Details account security and password guidelines	37.6%	5.4%	44.1%	6.5%	6.5%
Details network security and bandwidth guidelines	48.4%	3.2%	38.7%	5.4%	4.3%
Details early recognition of potential viruses attacks and phishing attacks	23.4%	2.1%	61.7%	8.5%	4.3%
Explains protection from identity theft	20.4%	4.3%	60.2%	9.7%	5.4%
Details academic integrity (digital plagiarism) and copyright guidelines	44.1%	22.6%	22.6%	5.4%	5.4%

Student Technology Standards

In the National C3 Survey qualitative interviews, tech coordinators and state directors indicated that Cyberethics, Cybersafety and Cybersecurity topics are addressed in the state and/or local student technology or media literacy standards. The existence of standards is backed up by other sources such as Education Week's *Technology Counts 2007 Report*, which indicated that the majority of states have adopted student technology standards—guidelines of what technology skills students should be aware of and what they should be able to do with technology. Only Iowa, Mississippi, and the District of Columbia did not, at the time of the report, have student technology standards in place. Out of the total, sixteen states have integrated technology within the standards of other content areas, while thirty-two states have adopted stand-alone technology standards.[xxxii]

As described above, LEA technology coordinators and state technology directors point out that Cyberethics and Cybersafety content are addressed at least briefly through these standards. However, as noted in the *Technology County 2007 Report*, few states assess students' skills. In fact, at this time, only four states actually assess students' competency of technology standards. One state director wrote, "We have not assessed students." Many educators confirmed this opinion, as one educator commented similarly, "for students, student knowledge is not assessed." Another noted, "Our state assesses students' competencies, but the focus has been on technology skills application." The No Child Left Behind Act (NCLB) requirement for states to report on 8th grade technology literacy begins in 2009, so assessments should be increasing. However, will this assessment continue to focus simply on technology skills and ignore the fundamental ethical, safety, and security issues that have arisen with the growth of IT as the foundation of work and business? Will the ethical lapses that have affected companies from a financial perspective (e.g. Enron, World Com, and Tyco), be more prevalent in IT in the future? This survey may serve as a call to arms to fill the information and education gaps, help direct policy decisions in the future, and serve as a baseline for comparison to examine effectiveness of such programs.

Nationwide comparisons of technology assessment will be difficult as technology literacy is left up to individual states to define.[xxxiii] Student technology standards are an excellent starting point to share guidance in what students should be aware of and have competencies in. Unfortunately, as one technology coordinator stated, "Student technology standards related to C3 topics are broadly worded," giving room for wide interpretation. Following are some examples of the variation in standards:

Students will be able to identify legal and ethical behaviors when using information and technology:

- *Copyright laws and fair use guidelines*
- *Acceptable use policy*
- *Internet use*
- *Students will demonstrate and advocate ethical and legal use of technology and information.*

A student will operate and maintain technical equipment and the work environment safely following applicable industry regulations and guidelines.

A few offer more specific measurable objectives, such as:

Students will identify examples of copyright violations, computer fraud, and possible penalties.

- *Examples: unauthorized use, computer hacking, software piracy, virus dissemination, fines*

Students will cite electronic sources properly.

- *Example: using Modern Language Association (MLA) or American Psychological Association (APA) style manuals*

Students will practice responsible and appropriate use of technology systems, software, and information to include:

a) explain the purpose of and follow the acceptable use policy
b) work cooperatively and collaboratively with others when using technology
c) practice responsible use of technology systems
d) demonstrate proper care of equipment (such as following lab rules, handling equipment with care, appropriate printing of resources)
e) explain the potential harm of instructive applications (such as worms, viruses, spy ware, popup windows, etc) and safeguards for limiting exposure to these
f) use safe and correct security procedures (such as protecting password and user ID)

However, detailed objectives and indicators are not common. Instead, broad-stroke objectives related to ethics and safety are more common, with few addressing security.

C3 Instruction Based on Student Technology Standards

Classroom instruction is tied closely to standards and guidelines created by local and state educational departments. These standards are interpreted by the teachers and integrated into lesson plans. The National C3 Baseline Study wanted to examine how technology standards were translated into curriculum and what issues in each of the C3 domains coordinators perceived to be components of the student technology standards for their districts and/or state. Technology coordinators were asked: *If your county/district/school does have technology standards (or follows the state technology standards) for students which of the following Cyberethics, safety, and security topics are specifically addressed within those standards? Check all that apply.* (See Tables 3-9, 3-10, 3-11.)

Of the coordinators surveyed, 7.4% indicated that no Cyberethics issues were included within technology standards, 8.5% did not see the inclusion of any Cybersafety issues, and 8.5% did not see the inclusion of any Cybersecurity issues. Additionally, coordinators reported at the following rates that each of these topics were only peripherally covered: 20.2% (ethics), 21.3 % (safety), and 25.4% (security). Given the 21st century focus on technology, it is surprising that so many states and districts do not have technology standards which include these topics.

In Table 3-9, over half the technology coordinators indicated copyright (60.6%) and plagiarism (54.3%) information is included in their technology standards. Coordinators also indicated file sharing (44.7%), fair use (48.9%), posting incorrect/inaccurate information (45.7%), stealing or pirating software, music, and videos (44.7%), cyberbullying (33.0%), and harassment (35.1%) were also included in standards. Given the high incidence of violations in these areas, and the countrywide interest and attention on these topics, it appears that inclusion in standards may be falling behind their prevalence.

Table 3-9 : [Coordinator Survey] Cyberethics Issues within Technology Standards

*If your county/district/school does have technology standards (or follows the state technology standards) for **students** which of the following Cyberethics topics are specifically addressed within those standards? Check all that apply.*	
Plagiarism	54.3%
Copyright	60.6%
Hacking	37.2%
Fair Use	48.9%
File sharing	44.7%
Cyberbullying	33.0%
Harassment	35.1%
Online etiquette protocols	37.2%
Posting incorrect/inaccurate information	45.7%
Stealing or pirating software, music and videos	44.7%
Online gambling	19.1%
Gaming	16.0%
Internet addiction	9.6%
State technology standards for students only peripherally address the cyberethics issues listed above	20.2%
State technology standards for students do not address cyberethics issues	7.4%

Table 3-10: [Coordinator Survey] Cybersafety Issues within Technology Standards

*If your county/district/school does have technology standards (or follows the state technology standards) for **students** which of the following Cybersafety topics are specifically addressed? Check all that apply.*	
Online predators	29.8%
Objectionable content	45.7%
Cyberstalking	21.3%
Pedophiles	12.8%
Hate groups	18.1%
Pornography	27.7%
Unwanted communications	35.1%
Online threats	28.7%
State technology standards for students only peripherally address the cybersafety issues listed above	21.3%
State technology standards for students do not address cybersafety issues	8.5%

Coordinators report that the inclusion of Cybersafety in technology standards is at troubling rates. As shown in Table 3-10, approximately 46% of respondents indicated objectionable content was addressed by technology standards. Particularly surprising, only one-third of coordinator respondents indicated that their technology standards addressed online predators (29.8%) and pornography (27.7%).

Continuing the downward trend, only 35.1% of respondents indicated viruses and self-replicating malicious code as topics included in student technology standards. Junk email

(25.4%), spyware (22.3%), adware (13.8%), phishing (19.1%), and pharming (2.1%) are included at surprisingly low rates. The dangers these techniques pose is substantial; their omission from standards should serve as a call to action to update the standards which ignore these critical topics.

Table 3-11: [Coordinator Survey] Cybersecurity Issues within Technology Standards

*If your county/district/school does have technology standards (or follows the state technology standards) for **students** which of the following Cybersecurity topics are specifically addressed? Check all that apply.*	
Hoaxes	23.4%
Viruses And Other Malicious Self-Replicating Code	35.1%
Junk Email	25.5%
Chain Letters	21.3%
Ponzi Schemes	2.1%
Get-Rich-Quick Schemes	3.2%
Scams	13.8%
Criminal Hackers	16.0%
Hacktivists	8.5%
Spyware	22.3%
Adware	13.8%
Malware	17.0%
Trojans	17.0%
Phishing	19.1%
Pharming scams	2.1%
Theft of identity	18.1%
Spoofing	10.6%
Privacy	30.9%
State technology standards for students only peripherally address the Cybersecurity issues listed above	25.4%
State technology standards for students do not address cybersecurity issues	8.5%

Summary

The National C3 Baseline Survey data show that states and local education agencies, as viewed by survey respondents, place the majority of responsibility of conveying Cyberethics, Cybersafety, and Cybersecurity in the hands of educators. In practice, this responsibility was not necessarily evenly shared by all teachers. Some information, primarily ethical issues (copyright, downloading, and plagiarism), may be conveyed in Acceptable Use Policies and/or student handbooks; however, comprehending the information was left as an independent activity for the student. The policies were issued at the beginning of the year to the students, who were expected to read, comprehend, and agree to them on their own time. Coordinators provided insight into LEAs focus on more inclusion of policies within AUPs and student codes of conduct, but clearly this is not occurring universally. Data show that some items are included within AUP and student handbooks, but these discussions are limited to prohibitions—restrictions on the use of the schools IT infrastructure—and convey limited insights on the topics to the students. Educators did not feel that consequences for cyberethical lapses, such as plagiarism, were backed up by the administration, and therefore they were likely to either ignore, or give simple warnings to offenders. Approximately 50% of the respondents indicated there were no clear methods chosen by their school or school district to convey information on Cybersafety and Cybersecurity to students. Some educators stated that C3 education was not their job—their educational plates were already full.

In order to get a feeling for what topics must be covered, an excellent beginning is viewing school/school district technology standards. However, as discussed above, only 50% of the coordinator respondents indicated plagiarism, copyright, and fair use being specifically in-

cluded in their student technology standards. However, given the more limited nature of the coordinator survey (ninety-four respondents), additional research should be undertaken to better refine this information. Additionally, sixteen states do not have stand-alone student technology standards. Instead, technology standards are integrated within existing core curriculum standards, and may focus primarily on technology skills and application. Standards are one way school districts and states guide curricula information, but the general descriptions within standards are subject to interpretation. Since C3 is not addressed specifically, the perception is that C3 topics are not being addressed by standards, and therefore are not taught in the classroom.

Teachers perceive themselves as being the main resource for students in these areas. Almost all educators expressed a need for knowing more about all C3 domains for both personal and professional reasons, and most find sharing this information with students critical, as things happening outside of school impact school instruction. Additionally, while many feel this should be the parents' role, it is noted that not all parents understand the subject area (certainly many of these teachers are parents themselves), and many parents are completely uninformed of these topics. For example, several respondents shared that immigrants and children of immigrant parents are at a particular disadvantage.

This section has explored a baseline of instruction and information—what is happening in schools and the classroom. Where information is not being provided, this survey tried to identify why not. Since educators seem to be in the best position to provide this information, the survey asked the next fundamental question, *Do educators feel prepared for the task?*

ENDNOTES

[xxx] Federal Communications Commission Consumer Facts: Children's Internet Protection Act, *http://www.fcc.gov/cgb/consumerfacts/cipa.html*

[xxxi] Open Congress. H.R. 1120 – Deleting Online Predators Act of 2007. *http://www.opencongress.org/bill/110-h1120/show*

[xxxii] Education Week's Technology Counts 2007, *http://www.edweek.org/ew/toc/2007/03/29/index.html*

[xxxiii] Larura Ascione, 2006, "States erratic on IT Literacy," http://www.eschoolnews.com/resources/measuring-21st-century-skills/measuring-21st-century-skills-articles/index.cfm?rc=1&i=36920

4

How Well Prepared do Educators Feel to Inform their Students about C3 Related Topics?

As described in Section 3 of the C3 Baseline Study, respondents perceive educators as being the main source of Cyberethics, Cybersafety, and Cybersecurity (C3) training for students. Despite the inclusion of some C3 content in AUP and student handbooks, mostly related to Cyberethics, educators still list modeling and encouraging proper behavior as the predominant means for teaching this information to students in the long term. For effective instruction, teachers need to feel comfortable, if not fluent, with the material or else they will ignore, avoid, and/or miss opportunities to instruct on these issues in the classroom. Therefore, it is imperative we examine how comfortable educators are with the content, and how prepared they are to discuss C3 with students.

The C3 Baseline Survey sought to identify educator knowledge gaps in order to identify topics requiring new training initiatives. For training to be effective, it must leave the recipient feeling capable and empowered to pass this information on to others: coworkers, students and parents. By obtaining data exploring information gaps from the perspective of the educators, professional development and continuous training can be developed to have maximum impact.

This section reveals that educators do not feel prepared to talk to students about many Cyberethics topics, and are particularly troubled by and unprepared to discuss most areas related to Cybersafety and Cybersecurity. Over 60.0% of educators do not feel comfortable discussing how to detect and minimize computer virus transmissions, and 52% do not understand how to ensure a website is secure. Sixty-seven percent do not know how to update their virus, firewall, spyware, and anti-spam filters, and 52% did not know how to install operating system (O/S) and software patches. Additionally, some do not feel any responsibility to understand these items, as they believe these topics are the domain of the IT department. Over 25% are not at all prepared to discuss Cybersafety issues including what to do when receiving unsolicited emails, how to be safe in an online environment, how to protect oneself while on social networking sites and while chatting, and how to respond to cyberpredators. In fact, less than 32% feel comfortable sharing guidance on any of these issues. In the area of Cyberethics, surprisingly 75% are not comfortable discussing cyberbullying, and only 36% understood copyright and fair use. These numbers reflect an across-the-board disconnect between the information that research and industry believes needs to be delivered to our students, and the knowledge and ability our educators have to deliver it. Given the level of discomfort described by educators, one might assume that the current mix of training is suboptimum, and/or current instruction is inadequate. Professional development opportunities will be discussed in Section 5.

The questions examined in this section were asked of educators with the following guidance:

Although not a part of your curriculum, if necessary or if the issues arise, how well prepared are you to talk about the below items. Rate each item on a scale of 1 to 5 with 1= Not at all prepared (I'm not sure what to tell

students. I would feel uncomfortable sharing guidance in this area) and 5 = very well prepared (I would feel comfortable sharing guidance in this area).

Thus we were not looking for "experts." These questions were seeking to find out if teachers felt they had enough knowledge to take advantage of teachable moments to bring these issues to bear in the classroom.

Cyberethics

The first area under investigation in this section looks at aspects of personal behavior related to ethical choices of using technology. Cyberethics is the discipline dealing with what is good and bad, and with moral duty and obligation pertaining to online environments and digital media. Many studies[xxxiv] have focused on these areas, with significant focus on plagiarism and cyberbullying. Given the focus on these concerns, one would expect teachers to have been extremely well prepared to discuss these issues with their students. As shown in Table 4-1, teacher respondents, on average, did not indicate they would feel comfortable sharing guidance in this area.

Acknowledging the attention the topic has been given in the news, not surprisingly, educators were most comfortable discussing plagiarism and citation with their students, with a mean value of 3.34. However, given such media attention, it is surprising that the mean was not higher. When teachers were asked, *How often do you perceive each of the following occurring over the course of a year in your school* (1= very high occurrence, 5 = no occurrence), the mean for plagiarism was 2.39±0.065*, indicating they believed it to be a fairly common occurrence. In fact, of those respondents who expressed an opinion, 25.2% believed it was a very high occurrence. This supports findings from earlier studies indicating similar results. The Center for Academic

Table 4-1: [Educator Survey] Comfort with Cyberethics Issues

	How well prepared do you feel to inform your students about …	**Mean**	**±*[xxxv]**
CE-1	forms of cyberbullying, the legal protections from cyberbullying, and how to report it	2.14	0.072
CE-2	what they can download from social networking sites or webpages (i.e, files, videos)	2.28	0.060
CE-3	copyright laws as applied to digital media, electronic information, and downloading files	2.80	0.065
CE-4	copyright laws as applied to educational uses (Fair Use)	2.98	0.065
CE-5	consequences of plagiarism	3.34	0.065
CE-6	how to correctly cite references	3.34	0.065

** $p<0.05$*

demic Integrity Study: *Student Cheating in American High Schools* reports that nearly 75% of high school students admitted to academic dishonesty.[xxxvi] Fifty-two percent stated they had copied a few sentences from a website without citing the source. The 2006 Josephson Institute *Report Card on the Ethics of American Youth* of 36,000 public and private high school students revealed one in three (33%) students admitted they used the Internet to plagiarize an assignment.[xxxvii] While educators felt most comfortable informing students about plagiarism and citation topics, one might expect the mean score to be higher than 3.34. Insight from the earlier section provides one explanation. Specifically, as stated in the quotes in Section 3, respondents shared that although policies might be included in student handbooks and Acceptable Use Policies

(AUP), in many cases, descriptions of violations and the associated consequences are not included. When educators identify a violation, students and parents complain, and often the school does not enforce follow-up. Since enforcement is uneven at best, many educators do not feel identifying violators is worth their effort, and therefore ignore or minimize the importance. In many cases they avoid discussing the topic. Some educators identified this as a predominant concern. As shared by one participant,

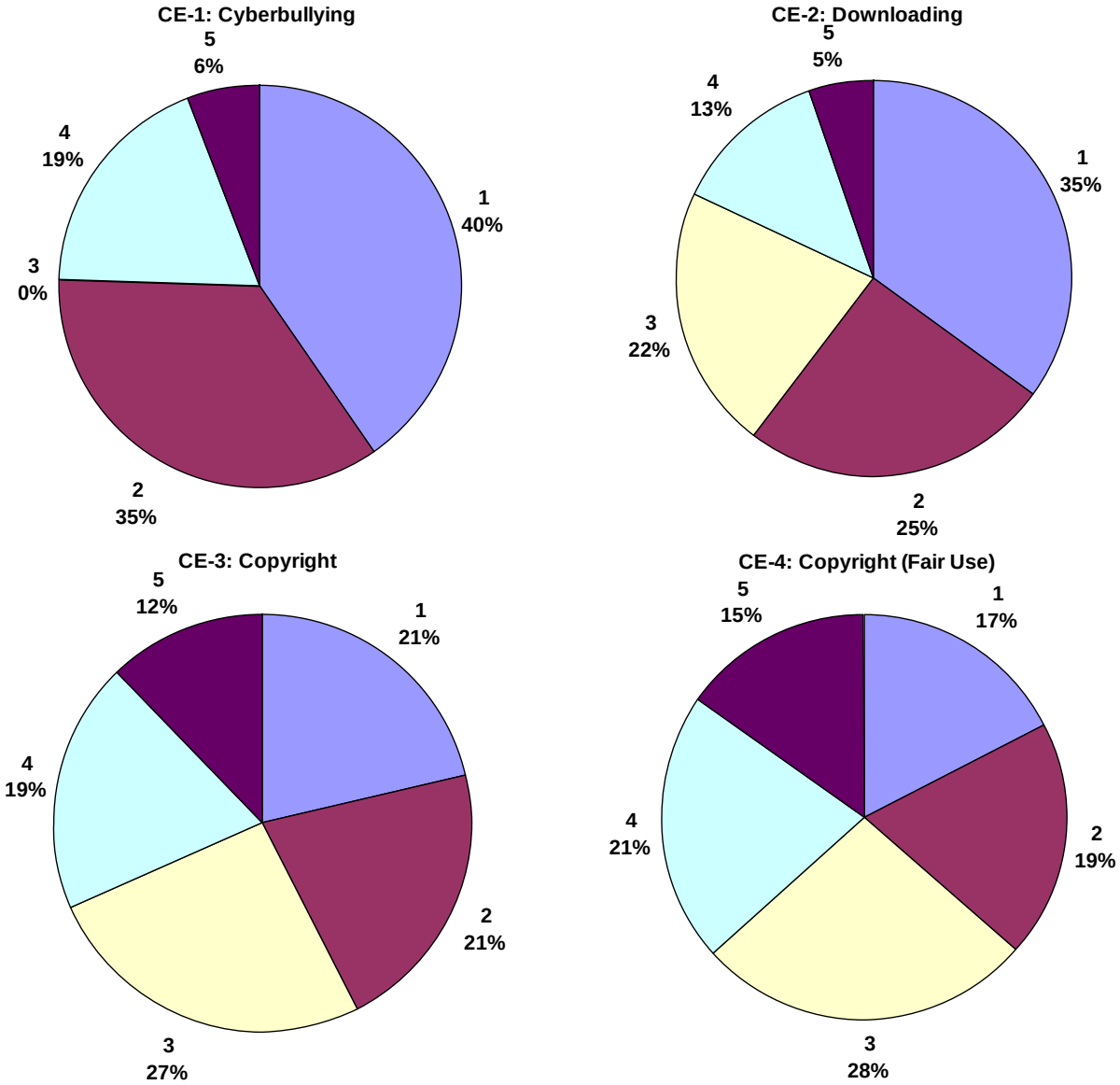
> *Plagiarism is the key issue with students of all levels. The computer has become a source of easy cut and paste. They DO NOT see the harm in this activity. We must change this; we need to encourage more creative writing; whether it is fiction or reporting facts. We must instill a sense of ownership of their own work, not that of others.*

This leaves educators in a quandary. The issue is important but unenforced, and may be part of their discomfort in discussing plagiarism more in depth.

At the other end of the scale, teachers were uncomfortable informing their students about cyberbullying (mean of 2.14, Table 2-1) and in fact, 75% indicated a comfort level of 1 or 2, signifying they were not prepared to share guidance in this area (see Figure 4-1, CE-1). This is also very surprising considering recent attention to this issue,[xxxviii] and calls into question the effectiveness of existing campaigns. Perhaps the campaigns are focusing predominantly on awareness, and are targeting students and parents. As one technology coordinator stated, "…when we had an Internet safety assembly, teachers spent most of their time disciplining students in the auditorium and didn't have much time to focus on the program itself ." Findings from this survey reveal that teachers do not feel they have the tools to discuss this issue.

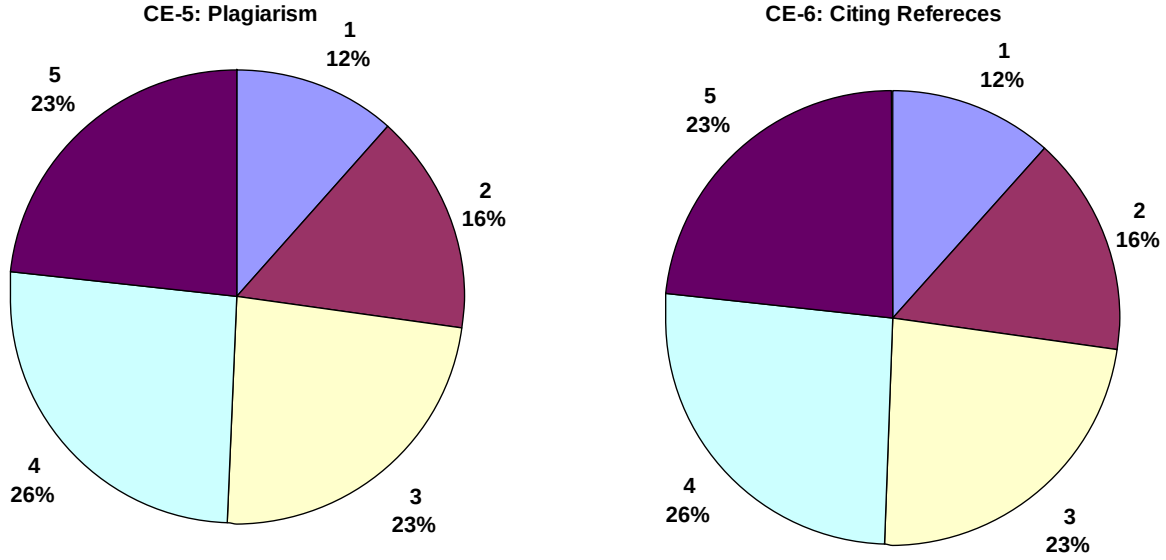
Likewise, survey data reveal that educators are not prepared to talk with students about what files are appropriate and safe to download from the Internet, and how to detect or avoid viruses, Trojans, spyware, or other malicious code. Only 18% of the respondents indicated they were prepared (4 or 5) to talk about this subject with their students. Copyright laws and their application to the classroom continue to be a point of confusion and consternation for teachers. Digital media is covered by copyright and numerous presentations have been given on the subject.[xxxix] Yet only 31% felt comfortable discussing copyright laws with respect to digital media (mean = 2.80), and only 36% felt comfortable discussing its application to education (mean = 2.98). As discomforting as this lack of Cyberethics knowledge is, educators were even more unprepared for Cybersafety issues, which is the subject of the next section.

Figure 4-1: [Educator Survey] Cyberethics - How well prepared do you feel to inform your students about …



1= Not at all prepared (I'm not sure what to tell students. I would feel uncomfortable sharing guidance in this area) and 5 = very well prepared (I would feel comfortable sharing guidance in this area).

Figure 4-1: (continued)



1= Not at all prepared (I'm not sure what to tell students. I would feel uncomfortable sharing guidance in this area) and 5 = very well prepared (I would feel comfortable sharing guidance in this area).

Cybersafety

Whereas Cyberethics focuses on the ability to act ethically and legally, Cybersafety addresses the ability to act in a safe and responsible manner on the Internet and in online environments. These behaviors can protect personal information and one's reputation, and include safe practices to minimize danger—from behavioral-based rather than hardware/software-based solutions.

In the area of Cybersafety, survey results indicate educators are still below the threshold comfort level of 3. As Table 4-2 shows, the average mean was 2.49 when asked how comfortable respondents would be sharing advice and knowledge to students about *how to protect from and respond to online cyberpredators, and identity theft.* As shown in Figure 4-2, only 22% felt comfortable (score of 4 or 5) with the subject. Similar results were shown when asked how prepared they felt to share guidance with students about *what precautions they need to take to avoid being a victim of cyber-crime* (identity theft, predators, cyberbullying, etc.) (M=2.46, 21% answered 4 or 5); *how they can protect themselves on social networking sites and while chatting* (M=2.46, 23% answered 4 or 5); and *strategies to protect personal information in online environments* (M=2.51, 23% answered 4 or 5). Slightly more positive results were returned for *what they should do if they receive unsolicited emails or instant messages* (M=2.68, 30% answered 4 or 5) and *requirements in creating a strong password* (M=2.72, 32% answered 4 or 5). Thus, in all cases, the majority of teachers did not feel they had the background knowledge to comfortably instruct their students on best practices. In fact, in all cases at least 25% of the respondents felt *Not at all prepared* to provide advice on the topic.

Table 4-2 [Educator Survey] Comfort with Cybersafety Issues

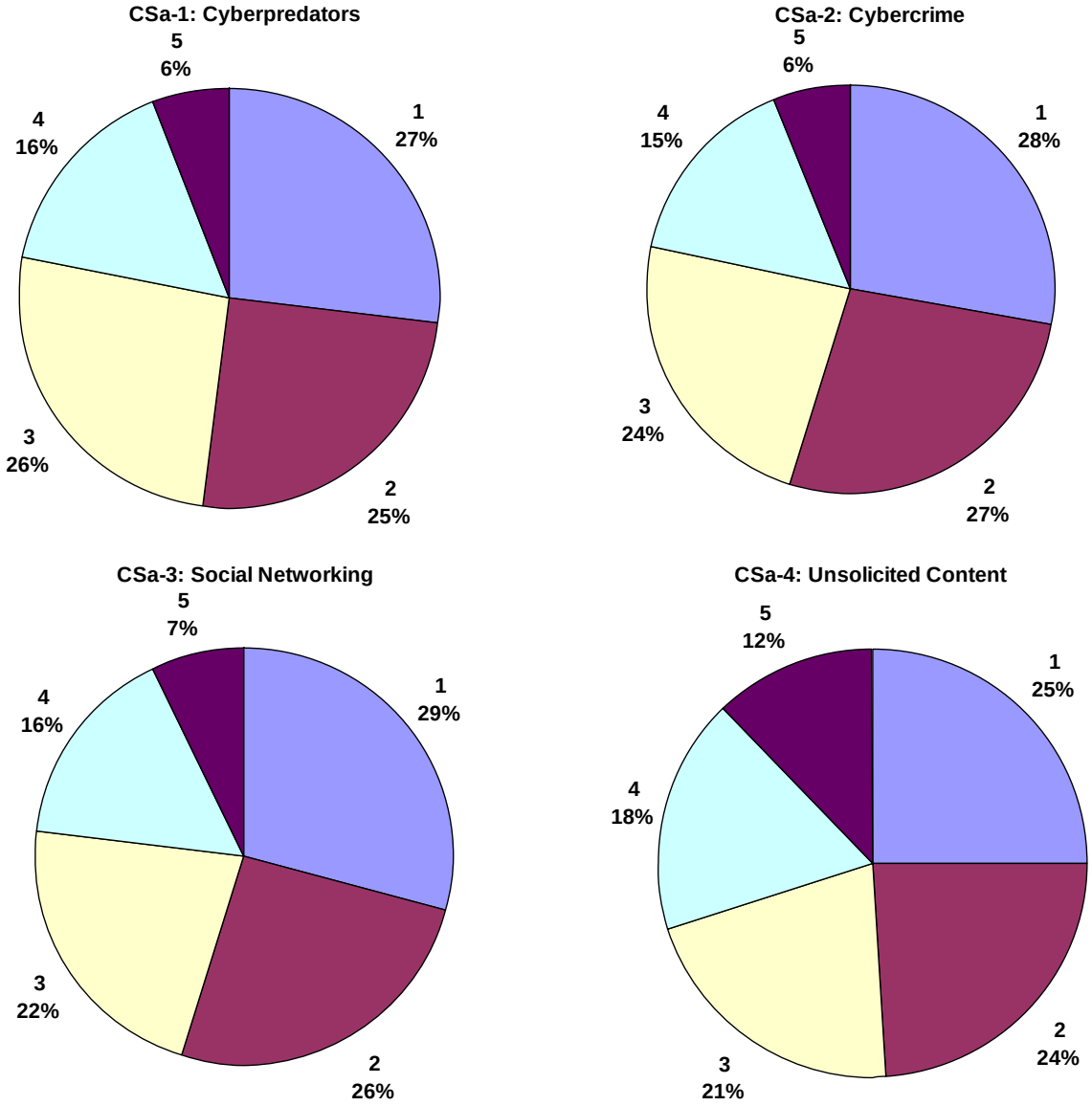
	How well prepared do you feel to inform your students about …	**Mean**	**±***
CSa-1	how to protect from and respond to online cyberpredators, and identity theft	2.49	0.060
CSa-2	what precautions they need to take to avoid being a victim of cybercrime (identity theft, predators, cyberbullying, etc.)	2.45	0.060
CSa-3	how they can protect themselves on social networking sites and while chatting	2.46	0.062
CSa-4	what they should do if they receive unsolicited emails or instant messages (information asking them to check out a picture, video or document, asking them to update account information or informing them they have won a prize)	2.68	0.067
CSa-5	requirements in creating a strong password	2.72	0.068
CSa-6	strategies to protect personal information in online environments	2.51	0.063

** $p<0.05$*

These results are alarming for several reasons. First, children are commonly instructed by public service announcements and new programs on TV, Internet information sources, safety literature, and Internet safety providers to confide in a trusted adult if any online activities make them feel uncomfortable. In addition to parents, educators are a critical group that children choose to confide in. Yet, educators clearly feel uncomfortable and ill-prepared to share insight on these topics. Secondly, Internet safety has been a major topic in the media, and several states have recently passed legislation mandating or promoting Internet safety lessons in the school setting.[xl] Cyberbullying has been a topic in both the news and in schools. However, these initiatives have not yet prepared educators to the level necessary for them to address the topics with their students. Perhaps lessons have been directed toward awareness for parents and students, and additional initiatives are required to address the educator component. When asking tech coordinators and state directors to comment on state and local Internet Safety initiatives and awareness programs, interview responses echoed these concerns, "Often one-time assemblies or general broad-stroke sessions are presented to teachers." "It's hard for them [educators] to take it all in one or two sessions and make sense." In almost all instances, state directors indicated that Internet safety awareness (as well as security and ethics) for students and teachers is under the directive of the local educational agency (LEA). Both tech coordinators and state directors also shared that LEAs are required to indicate in their local technology plan submitted to the state, how they will address Internet safety, or in some cases, cyberawareness, as defined by the technology standards. However, it was also revealed that implementation is left to the LEAs and not assessed.

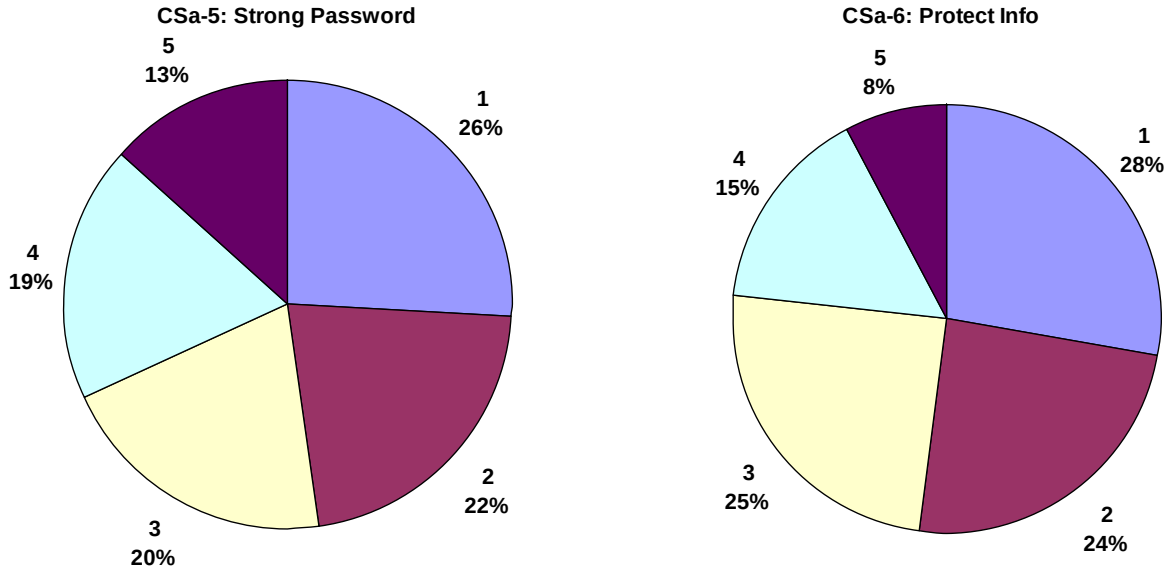
The graphs shown in Figure 4-2 specify the comfort level denoted by respondents with respect to the issues listed in Table 4-2. These results are particularly troubling as they suggest that, across the board, educators lack the necessary preparation to inform their students about these issues. As stated earlier, the highest competency, 5, was to designate *very well prepared (I would feel comfortable sharing guidance in this area),* and not *I am an expert (I can instruct at the highest levels).* The survey was directed to reveal the ability to inform and share, and the data indicates educators are not at the preparation level needed to share guidance. Unfortunately, comfort with Cybersecurity knowledge is even more distressing.

Figure 4-2 [Educator Survey] Cybersafety - How well prepared do you feel to inform your students about …



1= Not at all prepared (I'm not sure what to tell students. I would feel uncomfortable sharing guidance in this area) and 5 = very well prepared (I would feel comfortable sharing guidance in this area).

`Figure 4-2: (continued)



1= Not at all prepared (I'm not sure what to tell students. I would feel uncomfortable sharing guidance in this area) and 5 = very well prepared (I would feel comfortable sharing guidance in this area).

Cybersecurity

Cybersecurity is defined by the HR 4246, Cyber Security Information Act (2000), as "the vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems or other similar conduct that violates Federal, State, or international law, that harms interstate commerce of the US, or that threatens public health or safety." For the purposes of this survey, we define Cybersecurity to cover physical protection (both hardware and software) of your information and technology resources from unauthorized access taken by technological needs. In contrast, most of the issues covered in Cybersafety are steps that one can take by not revealing information by "social" means.

Cybersecurity is the area in which educators felt most uncomfortable giving advice to students. As shown in Table 4-3, the highest mean resulted when asking educators how well prepared they felt they were to *inform students about the importance of firewalls, virus protection, and anti-spyware to protect their information from compromise and identity theft*, but this question only had a mean of 2.60 on the 1-5 scale, and as shown in Figure 4-3, only 28% rated themselves with a comfort level at 4 or 5. The next highest mean resulted in their comfort in *informing students about spam, its characteristics, and avoidance*, which had a mean of 2.41, yet only 20% of the respondents felt comfortable discussing the topic (level 4 or 5). These two topics are not highly technical and merely are supposed to address an ability to provide a checklist of Cybersecurity needs, and warn of the associated dangers of not having these protections in place, yet teachers do not feel prepared to discuss these topics. In fact, for these subjects, 26% of respondents said they were *uncomfortable sharing information about firewalls*, and 31% were *uncomfortable discussing spam.*

Table 4-3: [Educator Survey] Comfort with Cybersecurity Issue

	How well prepared do you feel to inform your students about …	**Mean**	**±***
CSe-1	how to make sure a website is transmitting information securely	2.24	0.063
CSe-2	spam, its characteristics, and avoidance	2.41	0.061
CSe-3	the importance of firewalls, virus protection, and anti-spyware to protect their information from compromise and Identity theft	2.60	0.063
CSe-4	detection and minimizing computer virus transmission from both documents and email	2.29	0.061
CSe-5	the installation, configuration, and updating of firewalls, virus protection, spyware detection, and anti-spam filters	2.12	0.060
CSe-6	how to automate data backups	2.06	0.060
CSe-7	how to update operating systems patches, browser(s), and productivity software (i.e. email programs, office programs) to the latest version	2.27	0.082

** $p<0.05$*

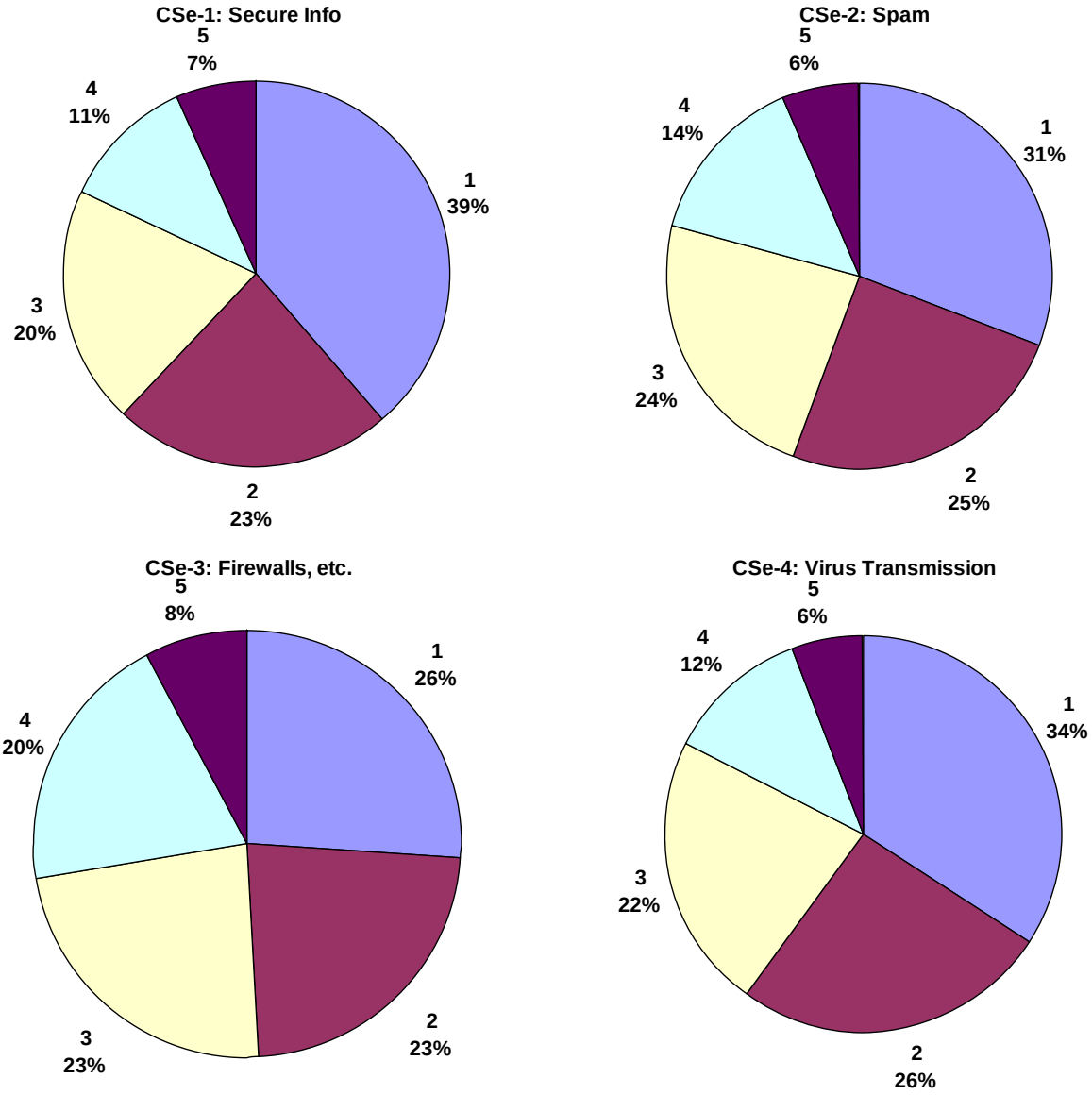
The discomfort respondents had discussing Cybersecurity topics extends to all questions in this area. Fifty-two percent of respondents could not discuss how to make sure a website was transmitting securely (level 1, 2); 60% could not discuss how to detect and minimize computer virus transmissions; 67% could not discuss how to update a firewall, virus, spyware, and anti-spam software; 52% could not discuss how to update operating system and software patches,; and 67% could not discuss how to automate backups. Educators seem to have relegated Cybersecurity solely to the domain of the IT department. Comments from respondents included, "Our tech department is usually responsible for the installation, update and purchase of all software and security issues with all computers used in the District. Also the training of any relevant material," and "Most of what you asked about does not really apply to classroom teachers. Leave the security to the tech support people." Thus, not only are some educators not informed about security, many do not see any need to be informed. Although school computers may be tied to a central IT support organization, many teachers either have a school-issued laptop, where, in many cases they can add/manage software, or a personal computer at home where they may be completing some of their school work. As the saying goes, forewarned is forearmed, and many teachers may be ignoring the warnings. With the greater assessment tasks being placed on teachers, we are not proposing that the computers be kept only at school—there is no way teachers could keep up. But instead, teachers must be made more aware of their responsibilities with regard to protecting the data with which they are entrusted and minimizing impacts from spam, pop ups, and spyware. Teachers must be urged to become knowledgeable citizens themselves, enabling them to convey that knowledge to their students.

As the use of laptops for teachers and students becomes more prevalent, one would anticipate security awareness to be a requirement. These survey results show otherwise. To see if this information tracks with the opinions of other educators, follow-up interviews were conducted with LEA technology coordinators and state directors. Findings complemented educator data. Both technology coordinators and state directors responded that much on the security side is managed by the LEA IT organizations, which aid in eliminating security mishaps. However, statements from educators indicate some major security flaws. "Yes, I have installed software and downloaded files

from home onto my laptop" and similar statements were common in the educator interviews. Although interviews and focus groups were only conducted with a select group and may not be a representative sample, the results from the survey indicate that this may be a more ubiquitous problem. Classroom teachers need to better understand their responsibilities as the front line of Cybersecurity. It should also be noted that Consortium for School Networking (CoSN) findings[xli] indicates a troubling concern, mainly with small school districts, of IT administrators being unprepared or not fully qualified. It was noted that many IT administrators lack background and professional knowledge in the domain of network security. Indeed, the concern has recently been raised with K-12 IT auditors.[xlii] One technology coordinator statement supports this argument, "…the IT admin person is a past science teacher who was interested in networking…seems to like it." This is consistent with the recently released Computing Technology Industry Association survey findings.[xliii] The 2008 CompTIA survey revealed a wide gap between IT security skills needed and those workers brought to the job. Forty percent of the organizations surveyed said their IT employees were "not proficient in such skills." Nearly three-fourths of the respondents specified security, firewall, and data privacy as the most important IT skills. However, only 57% believed their IT employees were proficient in such skills. They attributed this gap to the rapid change of technology, and sought to narrow the gap through training and incentives. Experience is not to be overlooked, however, as IT companies pointed out updated training and essential knowledge is indispensable. While not the purpose of this survey, several questions illustrate this point. When technology coordinators were asked *How often does your county/district/school require employees to change their passwords*, 38.6% indicated *only when forced to* and 25% responded *never;* when asked, *Is your technology acceptable use policy updated each year*, 26% responded *no.* Most businesses require strong passwords and changes every 90-180 days. The pace of change in technology is so fast, that yearly reviews and updates of AUPs are imperative. These findings indicate potentially severe security holes, and beckon further research to examine how pervasive these practices are and the security implications.

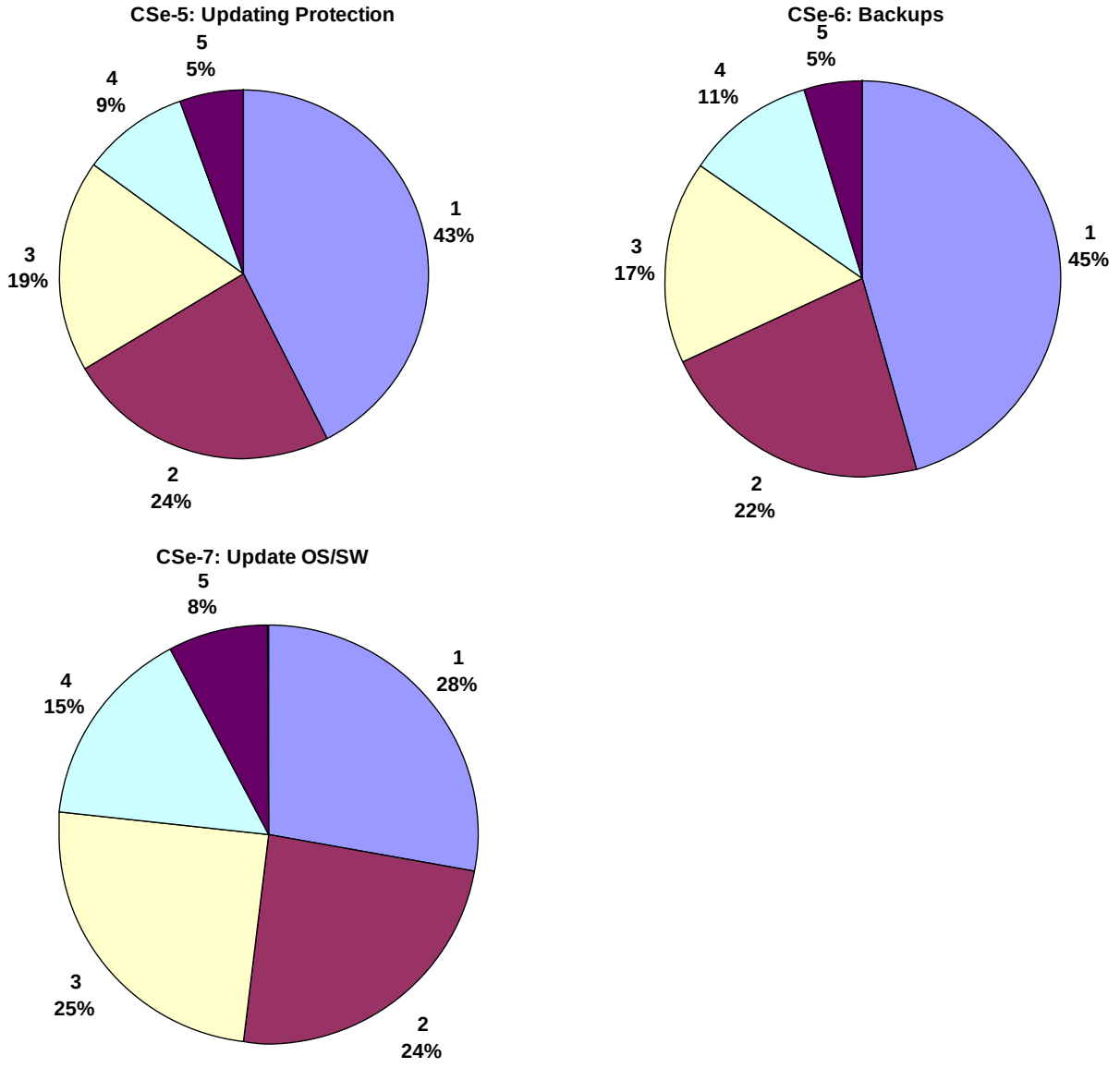
Educators are not merely the conduit of information; they are potentially vast consumers of technology. Professionally, online educational sites, educational and reference information, and web-enabled text books enhance the educational experience. Lesson plans and curricula are becoming almost exclusively produced on the computer. Productivity tools such as attendance, report cards, computer-based gradebooks, word processors, calendars, and email are the norm. Personally, most educators use cell-phones, cable modems, email, online stores, and distance learning to increase their knowledge. The productivity enhancement that technology provides, and the ease of producing metrics as required by NCLB, would seem to indicate a need to understand security. But instead, this is left to the domain of the IT department. However, business and government have already determined that security must be coupled with safe practices for maximum effectiveness. As shared by ISC^2's (International Information Systems Security Certification Consortium) security awareness campaign[xliv]: "Of all the scary things that can sabotage a network, human beings are by far the deadliest. In fact, *up to 80 % of security problems are caused by PEOPLE*. Instead of focusing on hardware and software solutions, we need to rely on another kind of security tool: *education*."

Figure 4-3: [Educator Survey] Cybersecurity - How well prepared do you feel to inform your students about …



1= Not at all prepared (I'm not sure what to tell students. I would feel uncomfortable sharing guidance in this area) and 5 = very well prepared (I would feel comfortable sharing guidance in this area).

Figure 4-3: (continued)



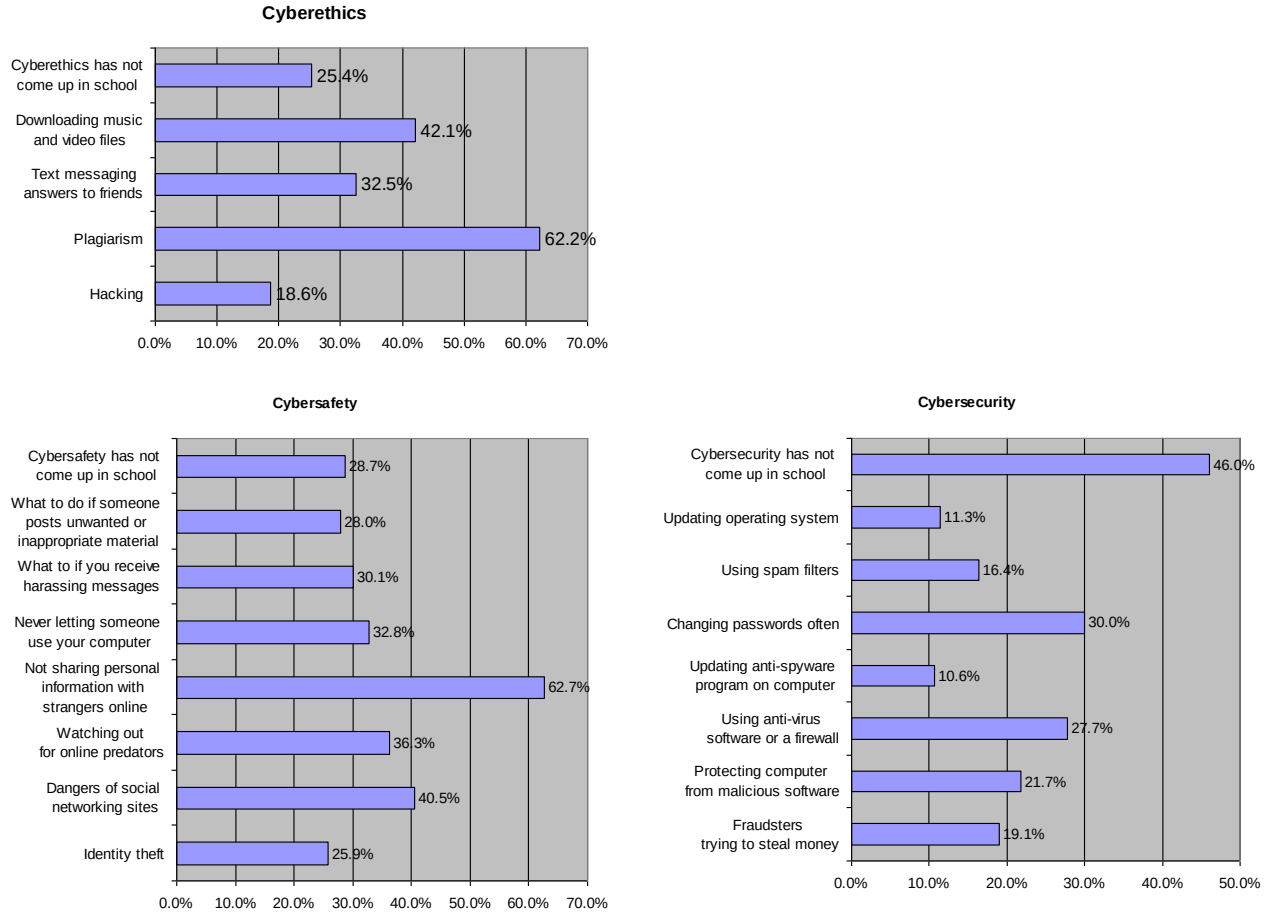
1= Not at all prepared (I'm not sure what to tell students. I would feel uncomfortable sharing guidance in this area) and 5 = very well prepared (I would feel comfortable sharing guidance in this area).

What C3 topics have come up with students, and what did teachers share?

Although the majority of educators surveyed did not feel well prepared to give guidance on C3 topics, during conversations and discussions with and between students, the topics have arisen. This survey investigated the topics that have come up most often in class. Additionally, although many educators did not feel comfortable giving guidance in many of the C3 areas, we were interested in knowing what comments, if any, did they share with students?

Figure 4-4 shows the C3 topics that have arisen in class. Not surprisingly, in the area of Cyberethics, 62.2% of educators surveyed indicated that the topic of plagiarism has come up in the classroom; 32.5% noted a discussion of text messaging test answers to friends had come up in class. Additionally, results revealed 42.1% responded that downloading of music and video files had presented itself. Surprisingly, 25.4%, a quarter of the educators surveyed, indicated that Cyberethics (including plagiarism, proper citation, cyberbullying, etc.) had never come up in class. In spite of studies indicating that approximately three out of four high school students have admitted to academic dishonesty, 398 out of the 1, 569 survey respondents have never had a chance to discuss this topic. Interestingly, this number is close to the 23% who had indicated discomfort with discussing plagiarism and proper reference citation in Figure 4-1. This begs the question, did the opportunity not arise, or did the educator intentionally avoid such a topic? In the interviews, one educator shared, "it's just so easy for students to take advantage of their tech know-how …I hear them talking about text messaging their friends about test questions …I haven't seen any in my class but that doesn't mean it hasn't happened." "It's easy to tell students they need to cite their resources, but I'm not sure I would really know the correct way to do it. I'd need to go back and brush up….most of this [citation process] is handled by the media specialist or English teacher." Only 18.6% indicated that hacking had ever come up in class in spite of the fact that several educators mentioned, in their comments and interviews, instances of student intrusion. For example, "Recently, our school district (the high school that our middle school feeds to) had a student break into the system and change student grades. It made big headlines!" Another teacher shared, "One of our students was able to send out a message to all staff [via one of the school's computers]…we were able to track down the student, by figuring out which computer it came from. But only because that computer was only used by two students, and one of them was absent on the day it was sent."

Figure 4-4: C3 Topics that Arise in School



The data shown in Figure 4-4 indicate that 62.7% of educators have had the topic of sharing personal information with strangers online arise in class. This is not surprising given the fact that the Pew Internet & American Life Project reports that 35% of all online teen girls blog, as do 20% of online boys; 54% of girls using the Internet post photos online, as do 40% of online boys.[xlv] Additionally, 32% of online teens have been contacted online by a stranger, and 49% of those who have posted a photo online have been contacted.[xlvi] Surprisingly, 28.7% of the C3 Baseline Survey educator respondents indicated that Cybersafety has not come up in school. However, research indicates that 93% of teens use the Internet, and 55% of those use online social networking.[xlvii] Social networking has only come up in 40.5% of the classes, even though over 50% of each class is using such sites. It seems unlikely that no Cybersafety topics have ever come up in the 28.7% of classes where teachers saw no opportunity to discuss the issue. Instead, there is a real concern that they cannot recognize the opportunity, or they actively avoid the discussion as they feel unprepared to share insight.

Also shocking is the fact that Cybersecurity has not come up in the classrooms of almost half (46%) of the respondents. Teachers may not understand the dangers of poor security, as only 30.0% have discussed password

changes, only 27.7% have discussed updating anti-spyware programs, and only 11.3% have discussed updating operating system software. When technology coordinators were asked *How often does your county/district/school require employees to change their passwords*, 38.6% indicated *only when forced to* and 25% responded *never*. This could represent a potential security concern. As mentioned previously, when asked *Is your technology acceptable use policy updated each year*, 26% responded *no*. Thus, the AUP may not include new and emerging dangers and threats.

As a follow-up question, we probed educators to reveal what information they shared when the topics did come up. In many cases teachers mentioned that they did not say anything; the conversation was among students and they were just listening in. Others gave more detailed accounts. A sample of descriptions provided by the respondents follows:

When ethical issues have come up in class I have shared with students…..

> *Taking things without permission, is like stealing (cutting and pasting).*
>
> *You need to use your own words and include references.*
>
> *When you cheat, you cheat yourself and others who have studied hard.*
>
> *Cyberbullying is just like bullying except it's online. Students need to ignore such behavior.*
>
> *You need to tell your student to talk to their parent.* [regarding inappropriate content placed in social networking sites]
>
> *I don't know what to say* [about cyberbullying]*…tell the administrator?*
>
> When Internet safety comes up in class I have shared with students…..
>
> *What I tell my kids is if they get strange emails or instant messages, they should just delete.*
>
> *… you can email back and ask to be taken off the list…*
>
> *Never trust anything you see.*
>
> *Never trust anything or anyone online.*
>
> *You need a least 5 letters and upper and lower cases.*

When Cybersecurity comes up in class I have shared with students…..

> *I don't order or bank online.*
>
> *You need to have anti virus software…although I'm not really sure what it is. But you need it!*
>
> *Never bank or order anything online…it's just not safe.*

Rather than learn safe practices, some teachers have taken a head-in-the-sand approach, and either avoided or lacked the opportunity to learn about technology, and are passing their lack-of-knowledge-based concerns on to the students.

Educator Comments about Need and Comfort Level

"I am not knowledgeable about any cyber topics"

Cyberethics

"I feel OK talking to students about plagiarism…but…."

- *"no real consequences for students if you do turn them in"*
- *"…usually have to handle it yourself. If you do something the parents complain"*
- *"cutting and pasting has just become so easy"*
- *"I reported a case to the administrator but because it would effect the student's playing* [a sport] *nothing happened"*
- *"it* [reporting] *…an incidence was a nightmare…parents came in and legal threats… it just wasn't worth it"*

One comment summed up what several general classroom teachers shared

- *"It's easy to tell students they need to cite their resources, but I'm not sure I would really know the correct way to do it. I'd need to go back and brush up...most of this* [citation process] *is handled by the media specialist or English teacher."*

With respect to cyberbullying

- *"I have no idea. The whole thing seems out of control."*
- *"The thing I find most troubling at the moment on this topic is cyber bullying. A lot of it goes on outside of school hours and there is the opinion from many school administrators that it is therefore not the school's responsibility to deal with. These problems spill over into a child's school day too and it becomes our problem."*

Cybersafety

- *"I just can not keep up. They all have MySpace accounts and cell phones."*
- *"I am a guidance counselor/assistant director of a middle school. I would love to be more educated about these subjects."*
- *"I graduated from a counselor education program in 2006, but did not receive any formal training on these topics. I have attended conferences where these topics were offered, but always went to other topics (could only choose one and others were more applicable to elementary students)."*

Cybersecurity

- *" I really don't understand any of this"* [cybersecurity topics listed in survey]
- *" I really need to learn more about how to back up my own files and use …and update protection"*
- *"The whole thing* [cybersecurity] *is bothersome and overwhelming"*
- *" never bank or order anything online…it's just not safe"*
- *"Much of the programming at my district is out of our control and patches, firewalls and such are left to the technology support team."*

Summary

This section has described educators' discomfort with C3 issues and indicates they are not likely to share guidance with students on such topics in the classroom. In the case of Cybersafety, educators feel that they do not understand the rules of social networking and safe downloading. They believe Cybersecurity is the exclusive domain of their IT department. Educators are uncomfortable with Cyberethics issues; they do not really understand the intricacies of copyright and fair use, and do not feel their administration will back them up in instances of plagiarism. They are also very uncomfortable with the issue of cyberbullying. Clearly, this survey has spotlighted some significant gaps in educator C3 knowledge, and as a result students may not be receiving the information on the topics they need. But what are educational systems doing to fill that educator knowledge gap? The next section examines this topic: *How educators are informed about C3.*

ENDNOTES

[xxxiv] **For Cyberbullying** see: David-Ferdon, C., & Hertz, M. (2007, Dec.). Youth Violence and Electronic Media: Similar Behaviors, Different Venues. *Journal of Adolescent Health*, 41(6). Supplement 1, A1-A4, S1-S68. Hinduja, S. & Patchin, J. (2008). Offline Consequences of Online Victimization: School Violence and Delinquency. *Journal of School Violence*, 6 (3), 89-112. Hinduja, S. & Patchin, J. (2008). Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization. *Deviant Behavior*, 29 (2). Ybarra, M.L., Diener-West, M., & Learf, P. (2007). Examining the overlap in Internet harassment and school bullying: Implications for school intervention. *Journal of Adolescent Health*, 41(6)., S42-S50. Wolak, J., Mitchell, K., & Finkelhor, D. (2007). Does Online Harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts. *Journal of Adolescent Health*, 41(6). S51-S58. Opinion Research Corporation (2006). Cyber bully pre-teen. Available at: www.fightcrime.org/cyberbullying/cyberbullyingpreteen.pdf. Opinion Research Corporation (2006). Cyber bully teen. Available at: www.fightcrime.org/cyberbullying/cyberbullyingteen.pdf. Wolak, J., Mitchell, K., & Finkelhor, D. (2006). Online victimization of youth: Five years later. National Center for Missing & Exploited Children. Ybarra, M. L., & Mitchell, K. J. (2004). Youth engaging in online harassment: Associations with caregiver-child relationships, Internet use, and personal characteristics. *Journal of Adolescence*, 27, 319-336.

For plagiarism see: Braumoeller, B. & Gaines, B.J., (2001, Dec.). Actions do speak louder than words: Deterring plagiarism with the use of plagiarism detection software. *Journal of Political Science and Politics*. American Political Science Association, 34(4), No.4, 835-839. Goodwin, A. (2007). Exploring the relationship between moral reasoning and students' understanding of the honor code. Dissertation, University of Maryland. Callahan, D. (2004). The cheating culture: Why more Americans are doing wrong to get ahead. Orlando: Harcourt. Center for the Study of Ethical development. (2005). http://www.centerforthestudyofethicaldevelopment.net. Cummings R., Dyas, L, & Maddux, C.D. (2001). Principled moral reasoning and behavior of preservice teacher education students. *American Educational Research Journal*, 38, 143-158. McCabe, D.L. (2005). It takes a village: Academic dishonesty. Liberal Education. Summer/Fall 2005. McCabe, D. L. & Bowers, W. J. (1996). The relationship between student cheating and college fraternity or sorority membership. *NASPA Journal*, 33, 280-91. McCabe, D.L., Trevino, L.K. and Butterfield, K.D. (1999). Academic Integrity in honor code and non-honor code environments: A qualitative investigation. *Journal of Higher Education*, 70(2), 211-234

[xxxv] This survey was undertaken with approximately 1569 educators. A confidence interval was computed based on educator responses. Thus, from a statistical perspective, with a 95% probability, one could state that the true population mean is within **±*** of the reported mean.

[xxxvi] Center for Academic Integrity Study: Student Cheating in American High Schools. Donald L. McCabe May 2001 http://www.academicintegrity.org/

[xxxvii] Josephson Institute's 2007 Report Card on the Ethics of American Youth http://charactercounts.org/programs/reportcard/

[xxxviii] Major campaigns have come from sources such as the National Crime Prevention Council (http://www.ncpc.org/cyberbullying), the US- Computer Emergency Readiness Team (http://www.us-cert.gov/cas/tips/ST06-005.html), the National Center for Missing & Exploited Children (http://www.netsmartz.org/resources/reallife.htm), iKeepSafe (http://www.ikeepsafe.org/), iSAFE (http://www.isafe.org/), WebWiseKids (http://www.webwisekids.org/), Stay Safe Online (http://www.staysafeonline.info/) and WiredKids, Inc. (http://www.stopcyberbullying.org/)

[xxxix] For example, *Copyright Issues in the Digital Environment* (http://www.edtechpolicy.org/C32006/Material/Bonner/C3Conf10.6.06.ppt) , by Kim Bonner, Given at the 2006 C3 Conference (http://www.edtechpolicy.org/C32008/) , and *Copyright, Fair Use, and the Cultural Commons*,http://mitworld.mit.edu/video/469/

[xl] For example, Kentucky has sent a bill to its legislature on February 13, 2008 (House Bill 367), and Virginia (HB58 – Approved March 7, 2006), passed a law requiring students to be taught about Internet Safety, and in Illinois, The Kotowski Internet Safety Bill (Public Act 095-0509 095-0509 - http://www.ilga.gov/legislation/billstatus.asp?DocNum=1472&GAID=9&GA=95&DocTypeID=SB&LegID=29564&SessionID=51 states that each school may adapt an Internet safety curriculum and recommends 2 hours of Internet safety content per year; in New York Bill A08333 http://assembly.state.ny.us/leg/?bn=A08333&sh=t ; Texas SB 136 Internet Safety Curriculum and Texas HB3171 Internet Safety: makes available curriculum for use to schools http://www.capitol.state.tx.us/BillLookup/History.aspx?LegSess=80R&Bill=SB136 and http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=80R&Bill=HB3171)

[xli] Education Break Out Panel: 2007 National Cyber Security Awareness Summit. See also CoSN Cyber Security for the Digital District http://www.securedistrict.org/

[xlii] See CyberWATCH http://www.cyberwatchcenter.org/ Research/Resources

[xliii]Security skills of IT workforce lacking, survey finds. http://www.networkworld.com/news/2008/022708-security-skills-it-workforce.html and "Skills Gaps in the World's IT Workforce: *A CompTIA International Research Study*"http://www.comptia.org/sections/research/research%20docs/ITskillsStudySummary2-08.pdf

[xliv] ISC^{2-} is the non-profit global leader in educating and certifying information security professionals. Their certifications include CISSP, ISSAP, ISSMP, ISSEP, CAP, and SSCP. https://www.isc2.org/cgi-bin/index.cgi

[xlv] Teens and Social Media: http://www.pewInternet.org/PPF/r/230/report_display.asp

[xlvi] Teens and Online Stranger Contact: http://www.pewInternet.org/pdfs/PIP_Stranger_Contact_Data_Memo.pdf . the definition of stranger is important to note. As noted in the briefing footnote, About a third of online teens (32%) have been contacted by "someone with no connection to you or any of your friends", and nearly a quarter of those contacted say that they felt scared or uncomfortable as a result. Please note that this definition of stranger contact may include a range of direct and indirect communications, including but not limited to: social networking site friend requests, spam email, or comments on a personal blog or photo sharing site.

[xlvii] Teens and Social Media: http://www.pewInternet.org/pdfs/PIP_Teens_Social_Media_Final.pdf

5

Educator Professional Development

Previous sections of the Cyberethics, Cybersafety, and Cybersecurity Baseline Study summarized data findings from the C3 Survey which indicate limited awareness programs and policies for students as well as discomfort and a general lack of fluency for educators. This section examines how C3 training is being provided to educators through professional development opportunities and how that can be improved, from the perspective of educators and technology coordinators. Cyberethics, safety, and security content will not benefit students unless educators are prepared to deliver guidance and content with confidence and in a systematic and sequential fashion. Teachers must receive the training necessary to enable them to share information with their students. The best designed training course cannot be effective unless it is delivered in the manner best suited to the audience—educators—and educators have an opportunity to attend.

Highlights

- 90% of educators have received less than 6 hours of C3 professional development in the past 12 months
- 24.4% of educators are ***very dissatisfied*** with C3 professional development training, and only 5% are ***very satisfied***
- Educators are very interested in all three C3 disciplines but coordinators do not see the need for Cybersecurity training – *many think the IT department is responsible for Cybersecurity*
- Digital media are the preferred means to receive informal training
    - 69.2% of educators and 84.0% of technology coordinators prefer this mechanism

Educator View

Educators are constantly being bombarded by new requirements: new curriculum and new assessment criteria. The LEA delivers training, but how much of this training is in the area of Cyberethics, Cybersafety, and/or Cybersecurity? How much C3 training is self-directed? This survey examines such questions. Table 5-1 shares educator responses to questions regarding the total training time they have received on C3 issues, in the form of in-service education from their county/district/school, continuing education or self-directed learning, and from courses in which they earned college credit.

Table 5-1 [Educator Survey] Time in C3 Training

About how much total time you have spent on in-service education provided by your county/district/school in the last 12 months?					
	None	< 6 Hours	6-15 Hours	16-35 Hours	>35 Hours
Cyberethics	43.7%	47.0%	6.1%	1.6%	1.6%
Cybersecurity	42.5%	48.5%	6.3%	1.5%	1.2%
Cybersafety	40.6%	48.4%	8.3%	1.5%	1.2%
What is the total time you have spent on training and/or continuing education done on your own in the last 12 months? Include attendance at professional meetings, workshops, and conferences, but do not include formal courses for which you received college credit.					
Cyberethics	50.7%	32.1%	11.0%	3.5%	2.6%
Cybersecurity	49.5%	34.4%	10.8%	3.0%	2.3%
Cybersafety	48.2%	35.0%	11.4%	3.4%	2.0%
How much time from courses for which you received college credit have you spent on training and/or continuing education in the last 12 months? Typically a 1 credit course offering equates to 15 hours.					
Cyberethics	78.6%	10.9%	5.8%	2.2%	2.4%
Cybersecurity	80.4%	10.6%	4.8%	2.2%	2.1%
Cybersafety	80.4%	10.7%	5.1%	1.8%	2.0%

This data are also graphed in Figure 5-1. The data show that in-service training is used most often as the means to receive instruction on C3 issues, followed by continuing education (not for credit). Few educators take C3-related courses for college credit. Based on data from Section 4, which indicates 27.3-75.5% of teachers feel unprepared to share guidance with students on C3 depending on the particular topic, it is not surprising that over 40% of educators acknowledged they received no training in C3 topics. Comments reported by web-based survey respondents provided additional insight:

> *Very little information of this type is generally available to our school population, either teachers or students. Some individual teachers instruct students on copyright and citation issues. The IT department for the district handles all other technical issues with our computers and online usage, with little input from the staff.*

> *Because of the age of my students and my subject area, proper use of computers does not come up often. I have had occasion to talk to my students about appropriate websites and computer courtesy. My school district has done a good job of teaching teachers to use computers. It has done a lousy job of teaching cyberethics, cybersafety, and cybersecurity to teachers.*

> *Our district staff has had little technology training. Because we're small and rural, we contract for IT services through the _____. We presently have two teachers being trained as technology coaches, and have plans to address cyber security with the middle school students.*

> *Technology is growing faster than education or society can keep up with it. We are in desperate need of additional staff, professional development, and resources so that we can provide students the necessary skills to appropriately take advantage of the technology.*

Follow-up interviews with LEA technology coordinators and state directors mirrored several educators' comments.

> *There is just no money available for technology training anything.*

We definitely understand the importance, and if we had the funding to support training efforts we'd love to invest in the effort. But we are strapped.

What's possible is to ask locals to include how they will address it [C3 awareness] *in their educational technology plans, but implementation is left up to them… primarily because of the funding issues.*

What we've used is outside organizations …Internet safety providers…training. But these are somewhat limited. They share many resources. GREAT! resources. But it's the teachers' responsibility to take the time to go through all the material…and they just do not have time.

Some states have state, regional, or local conferences and webinars, which provide information on a wide range of current technologies and insight into future directions of technology. Some of these conferences have topics related to ethics, safety and security. But not all educators attend. "I've never been able to attend these [ethics, safety, security] sessions. I've always chosen other presentations." Others mentioned state-wide initiatives, usually through state attorney general offices, that provide Internet safety training through individual classroom visits, school assemblies and/or "Internet Safety Nights" for parents and teachers. Other states held state summits with guest speakers and panel members including representatives from state attorney general offices, police department staff, and members from each state's Internet Crimes Against Children Task Force.

Figure 5-1 [Educator Survey] Time in C3 Training

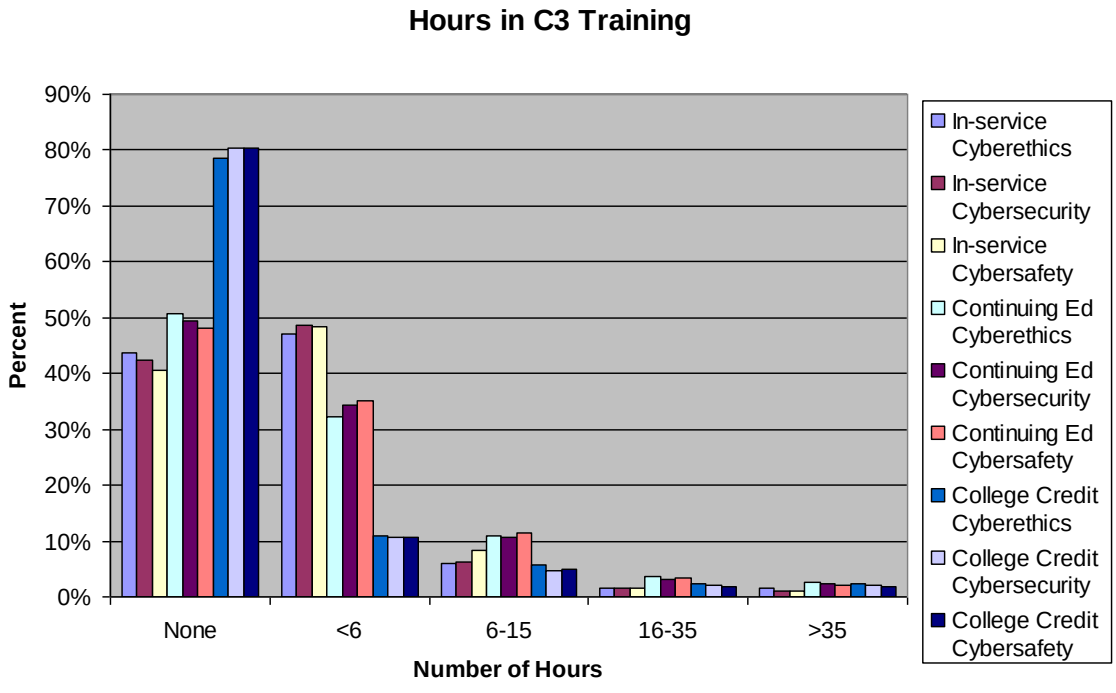


Table 5-1 and Figure 5-1 reveal very limited training on Cyberethics, Cybersafety, and/or Cybersecurity has been completed. Respondents were asked to comment on their overall satisfaction with the professional development they received. The survey selections were be-

tween 1 and 5, where 1 indicated *very dissatisfied*, and 5 indicated *very satisfied*. The mean responses are shown in Table 5-2. Overall, educators were *somewhat dissatisfied* with the training they received as indicated by the means ranging from 2.45 to 2.50. In fact, only 5% of all respondents indicated they were *very satisfied* with the training, and only 11.6% indicated a satisfaction level of 4. Qualitative interviews helped clarify the findings. "We had a half-day workshop on safety by an outside group. I just think I need more." "We were given a lot of great resources, but I need someone to walk me through." "I am just exhausted after school. We need several sessions...and more time." "Just seems like there is so much…you can't expect them to cover all of it in a half-day workshop."

Table 5-2 [Educator Survey] Training Satisfaction

Taking everything into consideration, please select the response which best describes your overall satisfaction with (1, very dissatisfied – 5 very satisfied)	
professional development by your school district/state regarding Cyberethics content	2.45 ±.055*
professional development by your school district/state regarding Cybersafety content	2.50 ±.057*
professional development by your school district/state regarding Cybersecurity content	2.49 ±.057*

*p< .05 Confidence Level

Although only limited professional development is currently available, teachers were very emphatic, both within their submitted comments and in the focus groups, about the importance of the topic, their desire to learn more for themselves, and the need to share this information with their students. The survey asked educators to list the degree to which they would be interested in learning more about the C3 topics listed in Table 5-3. Educators clearly have a strong desire to learn more about C3 issues. Within Cybersecurity, they are particularly interested in identity theft (76.9% indicated 4 or 5) and backing up files, firewalls, virus protection, anti-spyware, and anti-spam software (70.2% indicated 4 or 5). In fact, over 61.8% were interested (4 or 5) in all topics. In Cybersafety, 75.9% were interested in learning more about social networking safety, and 73.1% were interested in deterring and detecting online predators. Within this category, over 67.1% were interested in all topics. For Cyberethics, 75.8% wanted to learn more about helping students evaluate online content, and 70.3% wanted to learn how to detect and deter cyberbullying. In fact, only 5.7% overall indicated they were not at all interested (selection 1) in learning about these topics. Clearly, teachers are not comfortable with C3, but want to learn more about these issues. The educators were asked to list the priority of the professional development needs, from 1 (lowest) to 3 (highest). Most educators chose Cybersafety as their highest priority, with Cybersecurity second. Interestingly, 8.7% chose all three topics as highest priority, and 4.3% chose both Cybersafety and Cybersecurity as highest priority.

In addition to formal professional development, the survey questions asked educators by which informal means they preferred to receive C3 information. As shown in Figure 5-2, most educators (69.2%) prefer to receive updated C3 facts from digital media such as ezines, blogs, emails, and listservs. Second preference (at 46.7%, a difference of almost 23%), was through local newspaper and newsletters delivered to their home. Television advertisements (40.0%) and radio (36.6%)

were also seen as viable means to receive information, but local meetings and posters were not desired by many educators. Clearly, like the rest of the country, educators are moving online and use computer-based resources to keep up to date with information. In addition to hands-on and interactive training, it appears that a more focused digital media-based method may be a viable means to deliver information. This could be a tiered approach including a district/school C3 website, quarterly email newsletters, and an active listserv answering teacher questions. This type of approach can deliver continually updated material without consuming dollars for printing.

Table 5-3 [Educator Survey] Training Needs

Using the rating scale, please indicate the degree to which you would be interested in training in or materials to become more knowledgeable about: (1 – not at all, 5 – very interested)	
Professional Development: Cyberethics	
Promoting Academic Integrity (combating and detecting plagiarism, text messaging answers, using cell phones to send answers or take pictures of test)	3.65 ±0.062*
Deterring students from hacking	3.35 ±0.064*
Rules of Copyright and Fair Use	3.61 ±0.059*
Deterring and detecting cyberbullying	3.95 ±0.058*
Helping students evaluate online content	4.10 ±0.053*
Professional Development: Cybersafety	
Deterring and detecting online predators	4.05 ±0.057*
Filtering inappropriate content and Reporting illegal content, inappropriate websites and/or suspicious online behavior	3.85 ±0.058*
Helping students and parents understand safe and best practices in social networking sites	4.12 ±0.053*
Monitoring or awareness of sites for inappropriate content or danger signs (of suicide, huffing, etc.)	3.89 ±0.058*
Professional Development: Cybersecurity	
Identity theft	4.13 ±0.054*
Strong passwords	3.79 ±0.059*
Phishing and pharming scams	3.74 ±0.059*
Backing up files, and installing firewalls , virus protection, anti-spyware, and anti-spam software	3.93 ±0.058*
Reporting or next steps with suspected criminal activities on the Internet	3.79 ±0.058*

*$p<0.05$

Table 5-5 explores three major categories of professional development training: on-line modules, regional and university/local conferences and workshops, and in-district workshops. Regional, university, or conference workshops were given the least priority. Educators often find these difficult to attend due to a lack of funds for substitutes, travel, and conference fees. Further study is needed to see if making these opportunities more accessible would increase their relative preference. Looking at the means, more people preferred in-district workshops to on-line modules, although the difference was slight. In fact, if you look at raw numbers, more people listed on-line modules as their highest preference (735) than in-district workshops (722). Educators indicated they would prefer to receive additional training either as part of their current workday, or in a flexible manner they can complete when they have time available.

Figure 5-2 [Educator Survey] Informal Means to Receive C3 Information

C3 knowledge continues to change every day. By which of the following informal means do you prefer to receive updated information. (Multiple Selections Allowed)

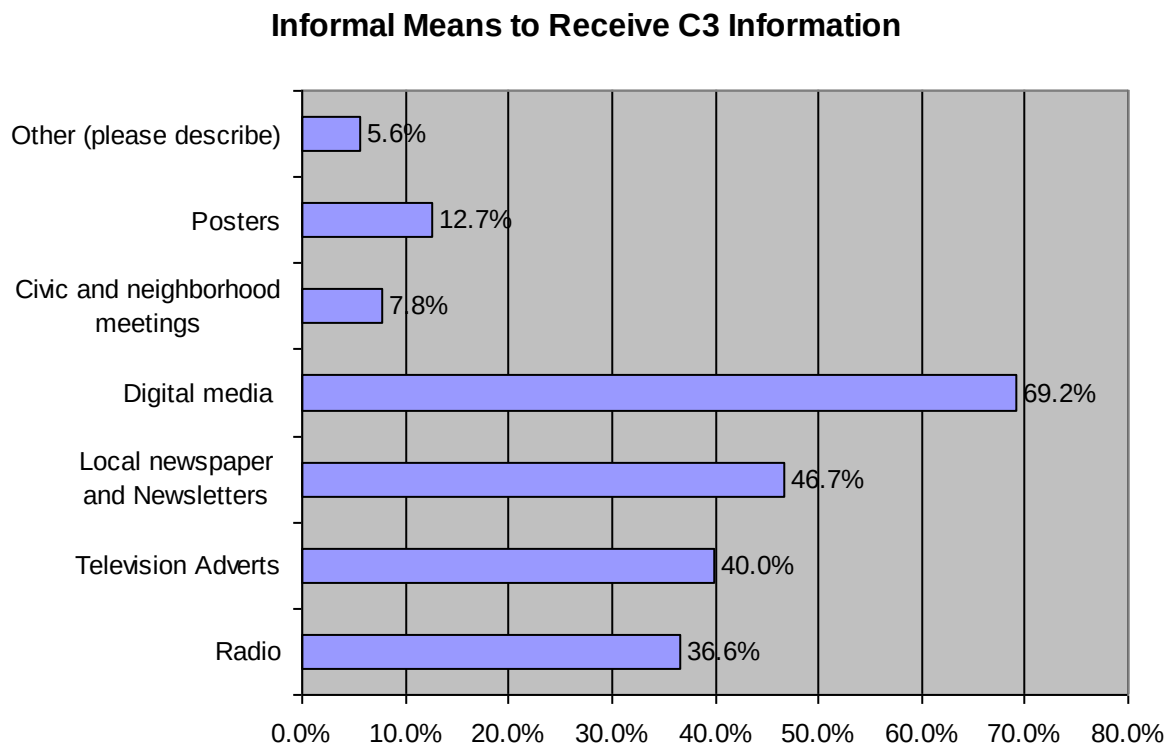


Table 5-5 [Educator Survey] Means to Receive C3 Training

Please rank the forms of professional development below from 1 (lowest) to 3 (highest) in order of your preference.	
On-Line Modules: This mode would provide on-line access to instructional programs that could be completed via computer any time	2.26±0.039*
Regional, University or Conference Workshops: This mode would make workshops available at various regional sites and conferences	1.73±0.035*
In-District Workshops: This mode would make training available to your district where teams of teachers from a school would be encouraged to attend	2.34±0.034*

*$p<0.05$

Coordinator View

The Cyberethics, Cybersafefty, and Cybersecurity (C3) Survey gathered data on professional development from LEA technical coordinators in addition to educators. Technology coordinators were asked similar questions, but from the perspective of the local education agencies (LEAs). What standards did they have? How do C3 topics trace to the standards? What means of delivery does the LEA focus on? What incentives are available for teachers to expand their knowledge? The intent was to correlate the responses from the educator survey (which were predominantly teachers), with the perspectives of technology coordinators who may have a higher-level perspective of available training. To provide context, coordinators were asked whether their district/school/county had technology standards for *teachers/educators* which covered technology uses and proficiencies. As Table 5-6 shows, 61.1% reported that there were standards, created either at the local or state level. This left 38.9% of coordinators, whose local professional development organizations had no technology standards, to direct professional development in any technology-based area. As professional development creation is fundamentally a result of content being directed by standards, and then budgeted accordingly, the result of these omissions will result in minimal training for those schools without standards. Much as NCLB has resulted in a drive to teach to assessments, professional development is often directed by standards.

Table 5-6 [Coordinator Survey] Teacher Technology Standards

Does your district/school/county have technology standards for teachers/educators (e.g., standards regarding proficiencies, uses of technology)? (N=94)	
Yes, our county/district/school has technology standards for teachers/educators.	40.0%
Yes, our county/district/school follows the state technology standards for teachers/educators	21.1%
No, our county/district/school does **not** have technology standards for teachers/educators	38.9%

Tables 5-7 through 5-9 list coordinators' responses regarding whether C3 topics are included in technology standards for teachers. In C3 topic areas, coordinators indicated a lack of coverage of C3 themes in their standards. The percentages varied from copyright (43.6%), down to Internet addiction (9.6%). Perhaps LEAs should examine where standards need to be refreshed (or reinterpreted) to include more of these important subject areas. Data indicate that teachers are not being informed about the different types of ethical issues that have arisen as the Internet and technology have become ubiquitous. With more and more of the data and systems being dependent on technology infrastructure, the lack of safety and security knowledge jeopardizes personal information for both teachers and students, and the LEA infrastructure as a whole.

Table 5-7 [Coordinator Survey] Teacher Technology Standards Topics: Cyberethics

*If your county/district/school does have technology standards (or follows the state technology standards) for **teachers/educators**, which of the following Cyberethics topics are specifically addressed within those standards? Check all that apply.* (N=94)	
Plagiarism	36.2%.
Copyright	43.6%
Hacking	25.5%
Cyberbullying	18.1%
Harassment	23.4%
Fair use	36.2%
File sharing	29.8%
Online etiquette protocols	28.7%
Posting incorrect/inaccurate information	18.1%
Stealing or pirating software, music and videos	36.2%
Online gambling	21.3%
Gaming	19.1%
Internet addiction	9.6%
State technology standards for students only peripherally address the cyberethics issues listed above	18.1%
State technology standards for students do not address cyberethics issues	4.3%

Table 5-8 [Coordinator Survey] Teacher Technology Standards Topics: Cybersafety

*If your county/district/school does have technology standards (or follows the state technology standards) for **teachers/educators**, which of the following Cybersafety topics are specifically addressed? Check all that apply.* (N=94)	
Online predators	16.0%
Objectionable content	33.0%
Cyberstalking	16.0%
Downloading	34.0%
Pedophiles	10.6%
Hate groups	20.2%
Pornography	28.7%
Unwanted communications	30.9%
Online threats	21.3%
State technology standards for students only peripherally address the cybersafety issues listed above	20.2%
State technology standards for students do not address cybersafety issues	5.3%

Table 5-9 [Coordinator Survey] Teacher Technology Standards Topics: Cybersecurity

*If your county/district/school does have technology standards (or follows the state technology standards) for **teachers/educators**, which of the following Cybersecurity topics are specifically addressed? Check all that apply.* (N=94)	
Hoaxes	21.3%
Viruses And Other Malicious Self-Replicating Code	34.0%
Junk E-mail	30.9%
Chain Letters	25.5%
Ponzi Schemes	6.4%
Get-Rich-Quick Schemes	9.6%
Scams	20.2%
Criminal Hackers	16.0%
Hacktivists	9.6%
Spyware	22.3%
Adware	18.1%
Malware	20.2%
Trojans	21.3%
Phishing	22.3%
Pharming scams	9.6%
Theft of identity	18.1%
Spoofing	12.8%
Privacy	27.7%
State technology standards for students only peripherally address the cybersecurity issues listed above	19.1%
State technology standards for students do not address cybersecurity issues	5.3%

As a decomposition of the teacher technology standards, we sought to find out how LEAs delivered C3 information to the teachers. As indicated in Table 5-10, close to half of all of coordinators surveyed (48.8%) indicated that C3 instruction is mentioned through other professional development activities. Thus, C3 subject matter was presented as one among several topics, and was not delivered with a particular focus on C3 alone. Only 9.3% had mandatory professional development dedicated exclusively to C3. The second highest percentage of educators, 38.4%, received information on C3 via flyer, newsletter, and website. Although these are often good means for dissemination, they are a one-way form of communication and lack the means for the recipient to ask questions and get clarification. Additionally, 33.7% of LEAs used county/district/school-sponsored workshops, and 25.6% used one-to-one and group training. Given the comfort levels described by educators in the section prior, one might assume that the current mix of training is suboptimum, and/or current instruction is inadequate.

Table 5-10 [Coordinator Survey] C3 Information Sources

How do most educators within your county/district/school system learn about C3 issues? (Choose the most common two)	
County/district/school sponsored workshops or seminars	33.7%
Mandatory PD days dedicated to C3 issues	9.3%
One-to-one or group training dedicated to C3 issues with technology coordinators or aides	25.6%
Flyers, newsletters, and websites	38.4%
Mentioned within other PD activities	48.8%
Workshops, seminars, and/or courses paid for by participants	16.3%
Other	8.1%

Table 5-11 examines how much time technology coordinators spent providing C3 professional development for their county/district/school. This chart indicates that 85.1% have spent less than six hours in Cyberethics training, 85.9% have spent less than six hours in Cybersecurity training, and 83.9% have spent less than six hours in Cybersafety training. This can be compared to Table 5-1, where educators indicate that in each of the C3 topics approximately 90% have received less than six hours of training. However, in Table 5-1, over 40% indicate receiving no training, whereas only 25% of coordinators have supplied no training. Since the coordinators are the ones delivering the training, and they may deliver it multiple times, it is not surprising that the coordinators indicate they have delivered more training than individual educators say they have received. In fact, one might have expected coordinators to have delivered even more training indicated This could be either because educators were using a broader definition of C3 training, or because a larger sampling of coordinators is needed.

Table 5-11 [Coordinator Survey] C3 Information Sources

About how much total time you have spent providing in-service education for your county/district/school?					
	None	< 6 Hours	6-15 Hours	16-35 Hours	>35 Hours
Cyberethics	25.5%	59.6%	11.7%	1.1%	2.1%
Cybersecurity	23.9%	62.0%	10.9%	0.0%	3.3%
Cybersafety	25.8%	58.1%	14.0%	0.0%	2.2%

Coordinators were asked what types of training have made the most significant impacts on teacher C3 education. Table 5-12 indicates that coordinators were unsure about many of the techniques, ranging from 9.4% to 26.7% (ignoring category "other"). Since coordinators should be most in tune with training effectiveness, it is troublesome that there was such a large group that was unsure of resource and training impacts. The table shows that coordinators identified the most significant sources of preparation as workshops and institutes, conferences, coaching and mentoring, teaching networks, individual/self-directed learning, and informal social networks of peers, family, and friends. Figure 5-3 plots the means of this data, ignoring "unsure" responses and the error bars indicating the $p<.05$ confidence intervals for this data. Other than the categories already mentioned, coordinators do not see these categories as significant sources for teacher training. Interestingly, although in Table 5-5 educators indicated they viewed conferences as the lowest priority means of obtaining C3 information, in Table 5-12 coordinators indicated it was a signifi-

cant means of obtaining information. Coordinators may have more exposure to conferences as a source of up-to-date information and the opportunity to interact with peers outside of the usual school environment. Whether conferences are more applicable to coordinators, or whether teachers need more opportunities to attend may be a subject for future study.

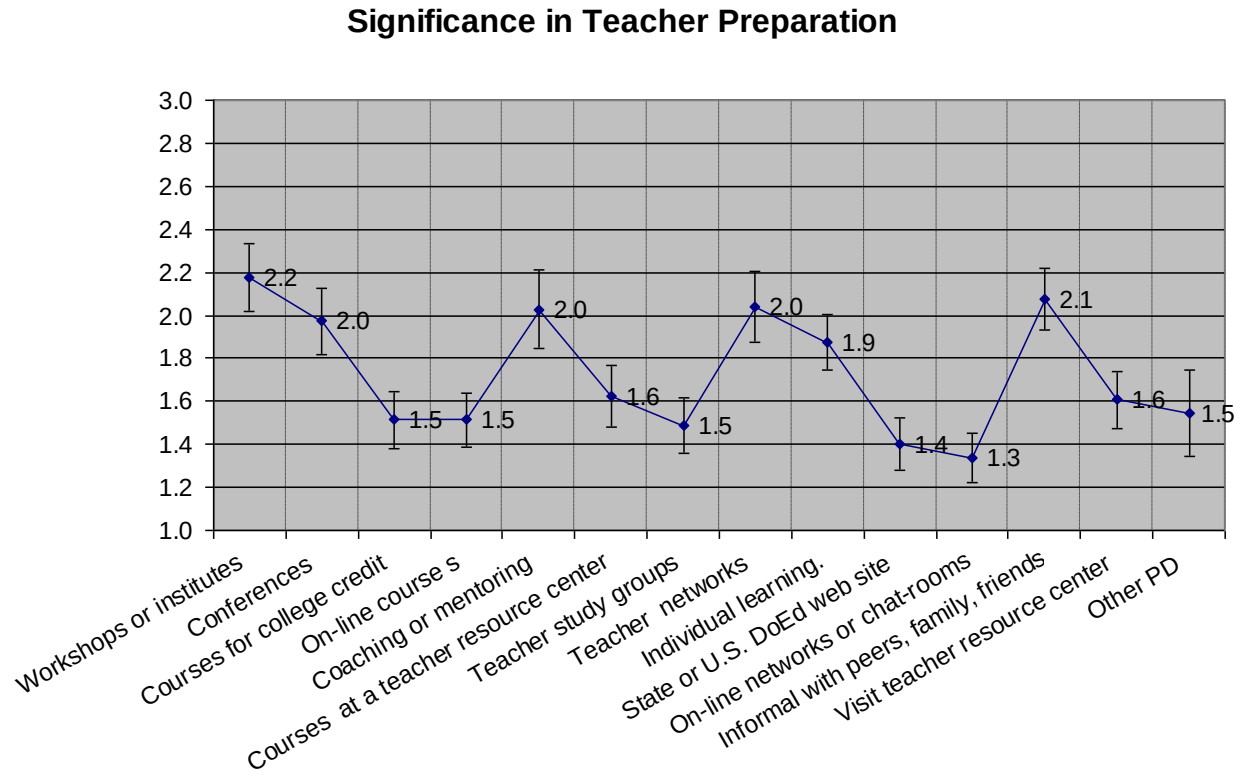
Table 5-12 [Coordinator Survey] Significance in Teacher Preparation

How significant a role have the following played in preparing teachers about Cyberethics, Cybersafety and Cybersecurity? (1 – not significant, 2, somewhat significant, 3 very significant, 4, unsure)

	(1) Not Significant	(2) Somewhat Significant	(3) Very Significant	(4) Unsure
Workshops or institutes	15.7%	42.7%	31.5%	10.1%
Conferences	24.4%	36.7%	22.2%	16.7%
Courses for college credit	47.2%	19.1%	10.1%	23.6%
On-line course participation	45.5%	27.3%	6.8%	20.5%
Coaching or mentoring arrangements designed to provide one-on-one technology-related instruction	29.9%	21.8%	32.2%	16.1%
Courses offered at a teacher resource center	40.0%	25.6%	11.1%	23.3%
Teacher study groups that meet regularly	43.3%	24.4%	5.6%	26.7%
Teacher collaboratives or networks	25.9%	35.3%	29.4%	9.4%
Individual learning in which teachers read journals or other professional publications, browse the Internet, etc.	21.1%	47.8%	11.1%	20.0%
Going to the State's or U.S. Dept. of Education's web site to get information/ materials	50.0%	18.9%	5.6%	25.6%
Participating in on-line networks or chat-rooms	52.3%	18.2%	3.4%	26.1%
Informally working with peers, family, friends and on skills related to technology in teaching	17.8%	45.6%	24.4%	12.2%
Visiting a teacher resource center which is staffed by lead or resource teachers and provides professional development materials/instruction	43.8%	28.1%	11.2%	16.9%
Other forms of professional development related to the use of technology in teaching.	43.4%	9.4%	13.2%	34.0%

Table 5-13 contains the mean and confidence intervals when coordinators were asked which topics their district would be more interested in learning about. Coordinators were most interested in learning about helping students evaluate online content, and helping students and parents understand safe and best practices in social networking sites. In Table 5-3, educators indicated a strong interest in Cybersecurity topics, but Table 5-13 shows a much different story. For example, the mean of the educator's survey was 4.13 for identity theft, 3.79 for strong passwords, 3.74 for phishing and pharming scams, 3.93 for backing up files, etc., and 3.79 for reporting criminal activities on the Internet. Coordinators, for the same subjects, answered 2.65, 2.71, 2.39, 3.01, and 3.36—a large difference. Although there were discrepancies between the other topics, it was most dramatic in Cybersecurity. Further investigation is needed to reveal the reasons behind this difference. It could be due to the fact that Cybersecurity is often described as the domain of the IT department, and as a result, coordinators are not interested in more training for their LEA. Teachers may feel that it is important for them to know more about the topics to be able to answer questions they receive from students, and for their own edification and use.

Figure 5-3 [Coordinator Survey] Significance in Teacher Preparation



Error bars indicated p<0.05

Coordinators were also asked to list their preferred means of C3 training from the perspective of the LEA. Similarly to educators, in-county/district workshops were the preferred means of information delivery, with online workshops listed second, and conference workshops listed third. This is interesting, as in Figure 5-3, conferences were listed as a significant method to use for training. This survey has revealed conflicting opinions on the value of conferences as a delivery mechanism for content. Further research may be needed, including a cost-benefit analysis of conferences for educators versus other delivery means. One option for leveraging conference budgets is for attendees to share what they learn with other colleagues as part of in-service presentations.

Table 5-13 [Coordinator Survey] Training Needs

Using the rating scale, please indicate the degree to which you and/or your district educators would be interested in training in or receiving materials on, to become more knowledgeable about: (1 – not at all, 5 – very interested)		
Professional Development: Cyberethics		
Promoting Academic Integrity (combating and detecting plagiarism, text messaging answers, using cell phones to send answers or take pictures of test)	3.39	*±0.298
Deterring students from hacking	3.13	*±0.267
Rules of Copyright and Fair Use	3.81	*±0.280
Deterring and detecting cyberbullying	3.74	*±0.268
Helping students evaluate online content	3.93	*±0.272
Professional Development: Cybersafety		
Deterring and detecting online predators	3.76	*±0.256
Filtering inappropriate content and Reporting illegal content, inappropriate websites and/or suspicious online behavior	3.87	*±0.277
Helping students and parents understand safe and best practices in social networking sites	4.06	*±0.250
Monitoring or awareness of sites for inappropriate content or danger signs (of suicide, huffing, etc.)	2.66	*±0.302
Professional Development: Cybersecurity		
Identity theft	2.65	*±0.273
Strong passwords	2.71	*±0.277
Phishing and pharming scams	2.39	*±0.298
Backing up files, and installing firewalls, virus protection, anti-spyware, and anti-spam software	3.01	*±0.269
Reporting or next steps with suspected criminal activities on the Internet	3.36	*±0.314

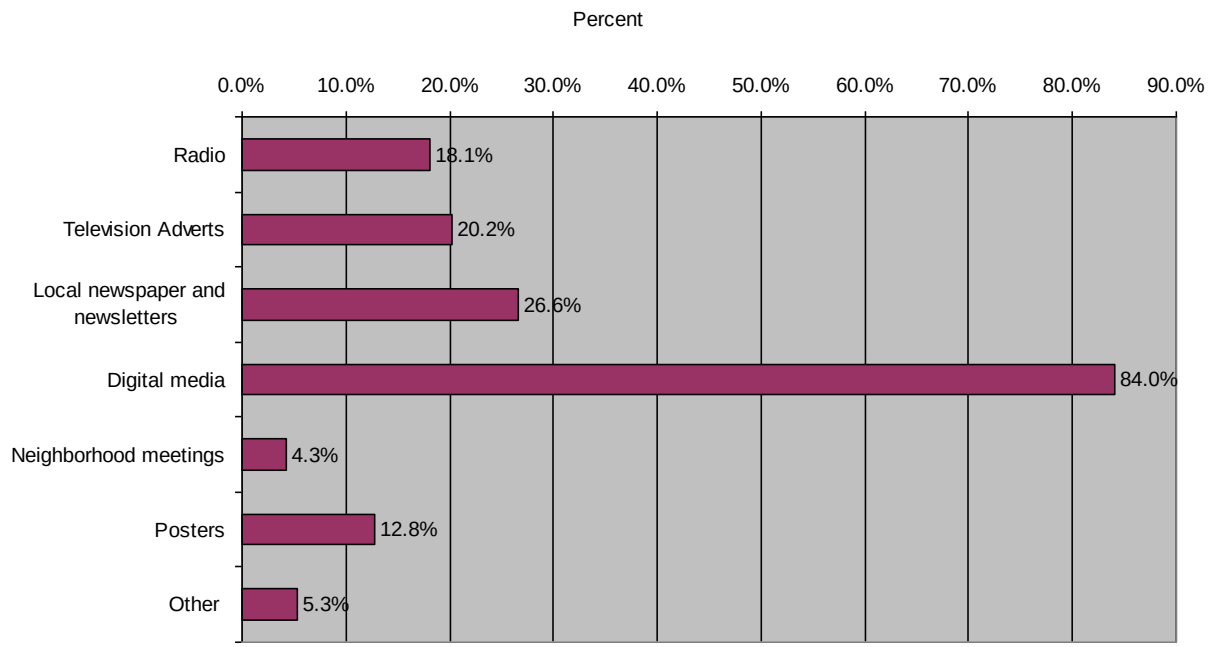
Similarly to educators, coordinators were asked by what informal means they preferred to receive updated information. The results are shown in Figure 5-4. The desire for delivery by digital media was even more pronounced for coordinators (84.0%) than educators (69.2%, see Figure 5-2). For coordinators, the next closest method was dramatically lower: local newspaper and newsletters at 26.6%. Clearly, of all informal means, coordinators prefer digital delivery. Although in Table 5-12, educators described conferences as having a significant role in preparing educators, in Table 5-14, they list conferences as the lowest priority form of delivering further content. Coordinators prefer to deliver content in-house, rather than have it delivered via outside means.

Table 5-14 [Coordinator Survey] Means to Receive C3 Training

If your county/district/school does feel the need for further professional development training in cyberethics, cybersafety and cybersecurity, please rank the forms of professional development below from 1 (lowest) to 3 (highest) in order of your school county/district/school preference.	
Online Workshops	2.17±0.136
Regional, University or Conference Workshops	1.49±0.129
In-County/District/School Workshops:	2.61±0.127

Figure 5-4 [Coordinator Survey] Informal Means to Receive C3 Information

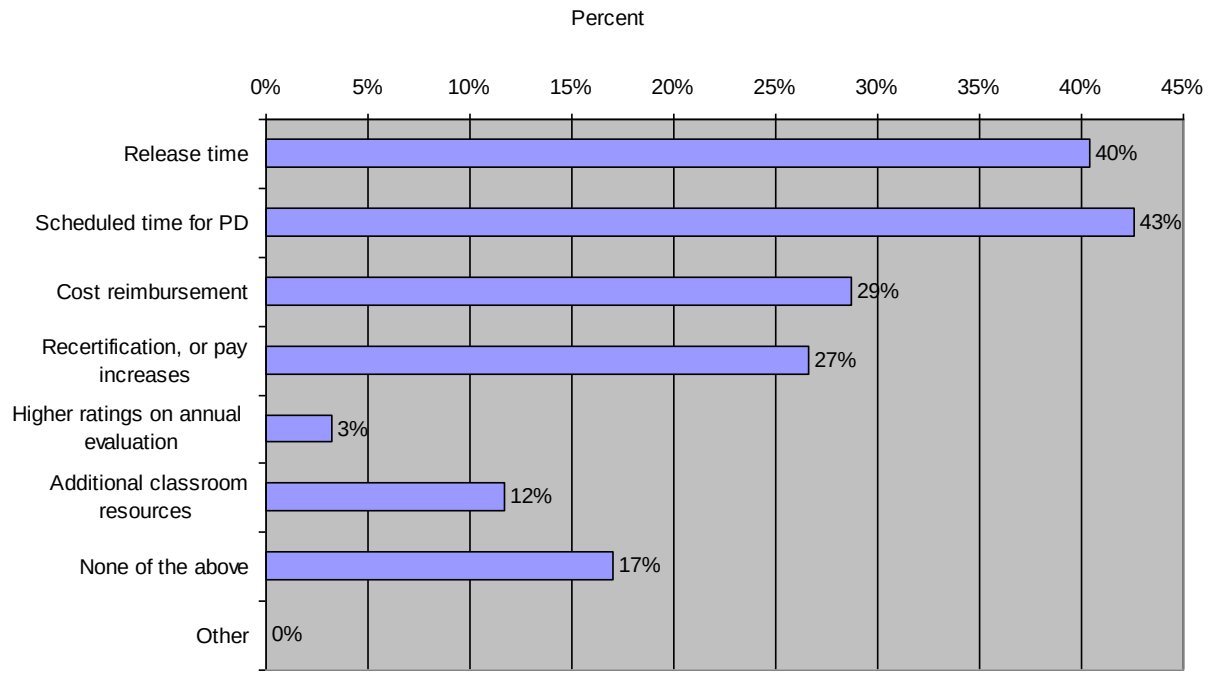
C3 knowledge continues to change every day. By which of the following informal means do you prefer to receive updated information. (Multiple Selections Allowed)



Coordinators were also asked what incentives are provided to teachers to assist them with C3 training activities. Their responses are shown in Figure 5-5. The two most frequently-cited incentives were release time and scheduled professional development time. The latter provides an opportunity to attend professional development activities in place of normal activities rather than adding to the educator's workload. Over one quarter of the LEAs also offered cost reimbursement for training, as well as pay increases and/or recertification credit. Only 3% of teachers would receive higher ratings on annual evaluations. In many companies, an increase in skills, and taking the initiative to get additional skills is reflected in the yearly evaluation. Apparently educators in LEAs represented in this survey did not have C3 professional development as part of their evaluation process.

Figure 5-5 [Coordinator Survey] Teacher Incentives

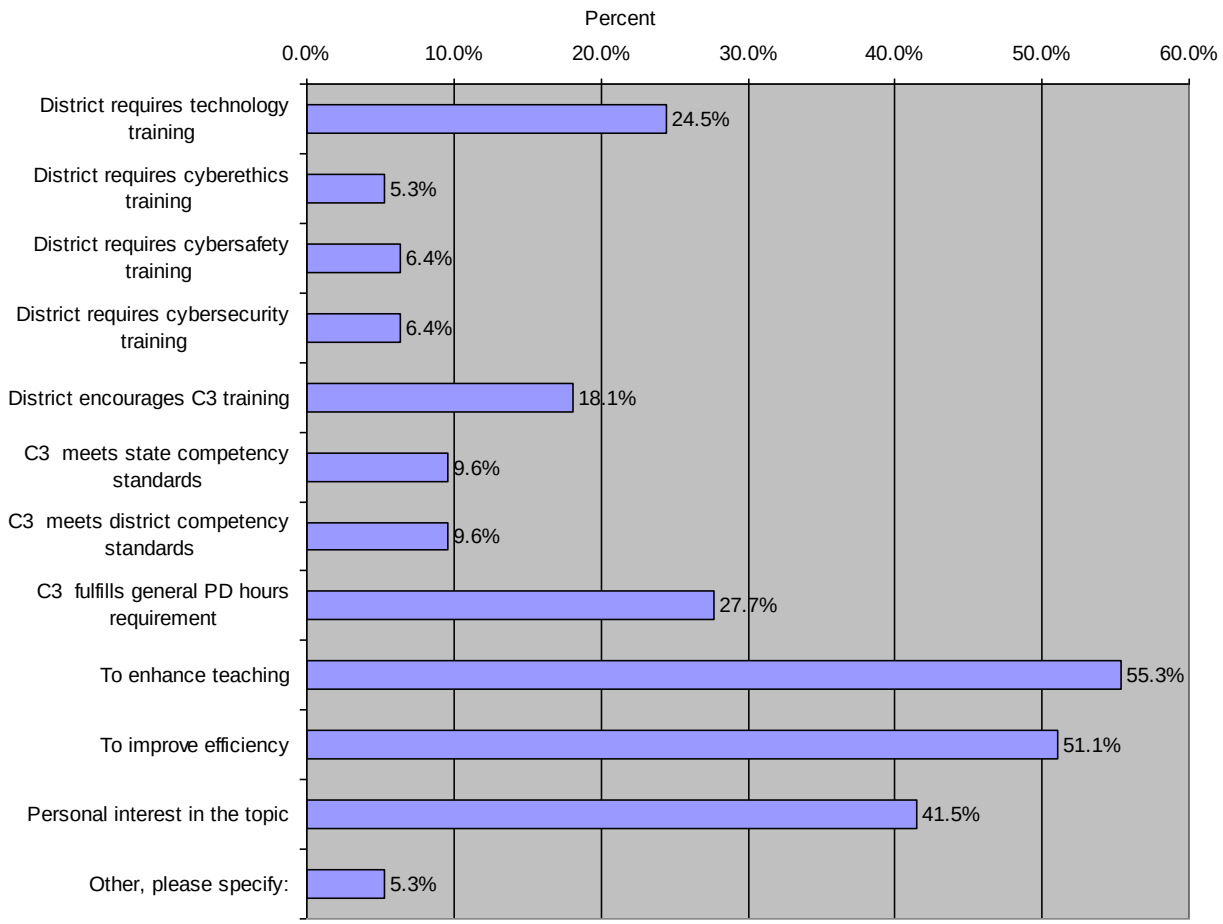
Which of the following types of incentives are available to your county/district/school's educators for participation in C3 educational technology-related professional development? (Check all that apply)



Coordinators were also asked to check the reasons that educators in their district choose to participate in formal and informal C3 professional development. The top three answers were related to personal motivating factors: to enhance teaching (55.3%), to improve efficiency (51.1%), and because of personal interest in the topic (41.5%). Approximately one-quarter indicated that C3 training was used to meet either general professional development requirements (27.7%) or more specifically, a technology training requirement (24.5%). Although some districts encouraged C3 training, this was judged by coordinators to only be a factor in 18.1%. Only 9.6% indicated training met state or district competency standards. Thus, although many teachers were self-motivated and took training to meet their own needs, the relatively few C3 professional development requirements may limit the number of teachers who actually pursue training activities on their own. If the requirements were increased, it is possible that additional training would be pursued.

Figure 5-6 [Coordinator Survey] Reasons for Pursuing

What are possible reasons for your county/district/school's educators participating in formal (educators themselves pay for course, conference etc.) and informal C3 educational technology-related professional development?



Summary

This section of the C3 Baseline Study examined both formal and informal C3 professional development activities from the viewpoints of both teachers and technology coordinators. Although teachers were told that Cybersecurity was the province of the IT department, and coordinators thought future training in this area was a very low priority, teachers still wished to expand their knowledge, both to teach their students and for their own edification. Professional development is often driven by state and LEA standards, and the limited C3-focused standards translated to limited C3-focused professional development opportunities. Instead, C3 was included within other training environments, although limited. Using a top-down approach (i.e. adding C3 to standards), or expanding the interpretation of existing standards, may result in an increased professional development focus on C3. This may expand the much-needed C3 professional development offerings. Additionally, both educators and coordinators expressed the fact that digital media was a preferred informal

means of receiving updated C3 information. LEAs could benefit from an increased focus on using this means to disseminate information as it can reach a large audience quickly, with minimal cost (no printing), and can also be used to provide information to both students and parents.

Appendix A

Acknowledgments

Educational Technology Policy, Research, and Outreach (ETPRO) would like to express our sincere appreciation to all of the contributors who made this study possible. Their contributions included brainstorming potential topics, reviewing and editing questions, participating and finding other educators to participate in the pilot test, facilitating recruitment efforts, logistics for state and LEA focus groups, and encouragement for the project. Your time, commitment, and expertise were very much appreciated. Additionally, all educators, technology coordinators and state directors of education who gave of their valuable time—we hope you hear your voices in this report and we hope the report helps you get the support for which you have asked.

Particular kudos go to Patricia MacDonald, Ray Meyer, Candace Caraco, Nancy Willard, Jim Teicher, Zulma Whiteford, and Jayne Moore for their candid suggestions and edits to the original questionnaire, Mary Ann Wolf and Tera Daniels from SETDA for their tireless efforts arranging focus group interviews with state technology directors, and Jayne Moore, Nancy Willard, Sandy O'Neil for final review. A special thank you goes out to the members of the ETPRO team, Bettina Grahek, Debbie McCauley, Andrea Bowers, and Clarise Jones.

Appendix B

C3 FRAMEWORK

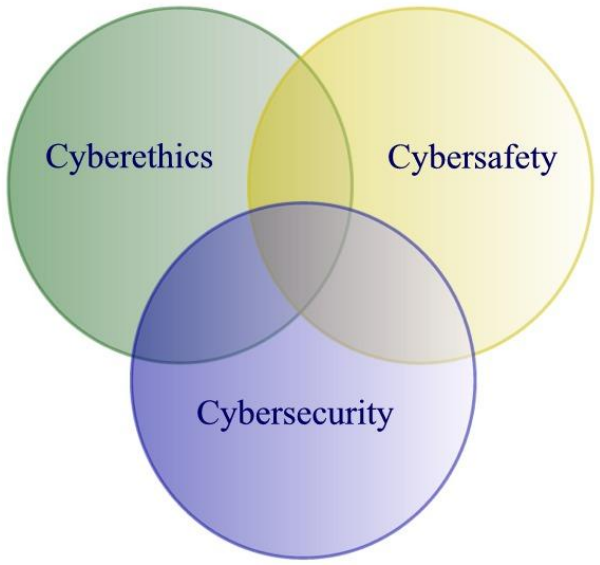
Promoting socially and ethically responsible use of technology is not a new phenomenon in education. Promoting responsible use has and continues to be acclaimed by many as a strategy under several brands to include *digital citizenship, cyberawareness,* and *cybercitizenship.*

Existing strategies of instruction include detailing student, teacher, and administration standards in AUP and student handbooks. Additionally, IT departments have installed Internet filtering and blocking software within state and local education agencies to ensure students' safe and secure technology use. However, some argue that having rules in handbooks and blocking/filtering content is not equivalent to safe practice instruction. Students need to understand the "why" behind the rules, and be able to institute best practices within their normal activities. Once students leave the school and are using unblocked, open systems, they are left unprotected and are not able to make the distinction between safe and dangerous practices. Additionally, practices do not include all Cyberethics, Cybersafety, and Cybersecurity (C3) topics and remain uncoordinated because state and local education agency standards use broad-stroke statements to guide competency. Interpretations of these standards or guidelines have in some cases missed the mark related to Cyberethics, Cybersafety, and Cybersecurity issues.

The Need for Developing a National Focus on C3

Many educational entities tend to pick and choose which C3 topics to teach, and often only talk about Cyberethics (e.g. plagiarism or cyberbullying). As revealed through survey findings, Cybersafety and Cybersecurity are virtually ignored in the educational setting, with the possible exception of a narrow focus on predators. Teaching to a C3 framework, where Cyberethics, Cybersafety, and Cybersecurity are taught as a whole, yet each having a unique focus, spotlighting the importance of each component, provides the opportunity for more complete coverage. Although clearly there is subject overlap (for example, one might need to learn security procedures to avoid having a computer vulnerable to an attack, and the ethical reasons not to "hack" into a computer to change grades), a separate focus gives rise to better appreciation of the appropriate uses of technology and does not negate the issues into one cloud labeled "Internet safety." By detailing particular elements under each domain, organizations can better design and address critical content. Teaching them as one, through branding such as *digital citizenship* or *Internet safety* curriculum makes it far

Figure B-1: C3 Framework: Learning Areas For Policy Development



too easy to check off the topic as "covered," while only scratching the surface of individual domains.

The presence of a policy framework can strengthen the already positive directions of Internet safety providers and state attorney general offices. Adopting a policy framework adds potential to broaden the impact on students, teachers, and parents in addressing ALL areas determined by government, business and industry, health agencies, and education to be of increasing importance. This model was originally conceived in 2000, and has become increasingly embraced and is the framework being adopted by the National Cyber Security Alliance, and several Internet safety providers and state educational agencies to guide the design of their policies, recommendations, and content.

What follows is a theoretical framework that can be used to inform a national, regional, or local agenda. It uses three dimensions, based on practical circumstances and experiences with educating students and teachers, with input from multiple stakeholders including parents, students, educators, technology coordinators, media specialists, curriculum resource teachers, Internet safety providers, and industry security specialists. The logo with its overlapping rings of Cyberethics, Cybersafety, and Cybersecurity indicates the subject areas have common ground, but have significant content that is distinct and must be discussed on an individual basis. Under each subject area, specific topics must be addressed. A brief synopsis of each area and associated topics are presented below.

Cyberethics

Cyberethics is the discipline dealing with what is good and bad, and with moral duty and obligation as they pertain to online environments and digital media.

Topics that might be included under this tenet are:

- Plagiarism
- Copyright
- Hacking
- Fair use
- File sharing
- Online etiquette protocols
- Posting incorrect/inaccurate information
- Cyberbullying
- Stealing or pirating software, music, and videos
- Online gambling
- Gaming
- Internet addiction

Cybersafety

Whereas Cyberethics focuses on the ability to act ethically and legally, Cybersafety addresses the ability to act in a safe and responsible manner on the Internet and in online environments. These behaviors can protect personal information and one's reputation, and include safe practices to minimize danger—from behavioral-based rather than hardware/software-based problems. Topics that might be included under this tenet are:

- Online predators
- Objectionable content
- Cyberstalking
- Harassment
- Pedophiles
- Hate groups
- Pornography
- Unwanted communications
- Online threats

Cybersecurity

Cybersecurity is defined by the HR 4246, Cyber Security Information Act (2000) as "the

vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems, or other similar conduct that violates Federal, State, or international law, that harms interstate commerce of the US, or that threatens public health or safety." Cybersecurity is defined to cover physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means. In contrast, most of the issues covered in Cybersafety are steps that one can take to avoid revealing information by "social" means.

Topics that might be included under this tenet are:

- Hoaxes
- Viruses and other malicious self-replicating code
- Junk email with links to malicious sites
- Chain letters
- Ponzi schemes
- Get-rich-quick schemes
- Scams
- Criminal hackers
- Hacktivists
- Spyware
- Adware
- Malware
- Trojans
- Phishing
- Pharming scams
- Theft of identity
- Spoofing
- Privacy

The topics listed above cannot be stagnant. Technologies are dynamic and ever changing. For example, cyberethical issues are experiencing vast transformation as a result of factors driven by the multi-media aspects of cell phones and the vast reservoir of information on the Internet. These factors include:

- The ease of cutting and pasting from the Internet and the growth of "paper-mills"
- Bullying taking on new dimensions through text and instant messaging, chat rooms, and postings on YouTube and social networking sites
- New ways to cheat—pictures of tests/quizzes to forward to friends, text messaging answers, and hacking into the school's computers to either download tests or change grades

Cybersafety, or the generic term *Internet Safety*, has received more public attention lately due to media coverage. The *To Catch a Predator*[xlviii] series on Dateline NBC has highlighted the problem of Internet predators and the dangers to today's user. In the 2005 Pew Internet and American Life report, *Protecting Teens Online*, 64% of online teens (ages 12-17) stated that they do things online that they wouldn't want their parents to know about, and 79% stated that they aren't careful enough when giving out information about themselves online. This has caused a recent movement of state attorney general offices focusing on safety awareness programs, many partnering with outside Internet safety providers like iKeepSafe,[xlix] iSafe,[l] and NetSmartz.[li] In many cases, usually due to time constraints, the focus has been on taking precautions while visiting social networking sites, limiting sharing of personal information, and an increase in "stranger danger" campaigns.

Only recently has Cybersecurity awareness in the educational setting made it on the radar screen. Yet, the Federal Trade Commission (FTC) reports that for the seventh year in a row, identity theft tops the list of consumer

fraud and identity theft complaints received and affects more than 10 million people every year, representing an annual cost to the economy of $50 billion dollars. Key findings from the 2007 CSI Computer Crime and Security Survey of IT security administrators (primarily government agencies) and large corporations found one-fifth suffered one or more kinds of security incident and most from a "targeted attack." Financial fraud overtook virus attacks as the source of the largest financial losses, and insider abuse of network or email edged out virus incidents as the most prevalent security problem. SANS listed web browser security, phishing and pharming attachments, and unencrypted laptops as just three out of twenty top security risks of 2007. For 2008, Georgia Tech's Information Security Center's top five emerging cyber threats included Web 2.0 and client-side attacks, targeted messaging attacks, Botnets, and threats to mobile convergence and Radio Frequency Identification systems. Google has stepped up its vigilance to report webpages that contain malware. Google estimates that more than 1% of all search results contained at least one result that point to malicious content[lii]. Denial of Service attacks, viruses, worms, Trojan horses, and computer fraud cost the country billions of dollars each year. Our youth (and educators) need to be informed about the dangers of not securing their personal information.

All of these challenges, if not properly addressed through a well-defined policy framework, can curtail the ability of all to effectively and safely utilize technology to its fullest potential in both the home and educational setting. The U.S. government has a National Cyber Security Division[liii] within the Department of Homeland Security to work collaboratively with public, private, and international groups to secure cyberspace and America's cyber assets. In order for the U.S. to remain safe and secure and not lose its competitive advantage in these fields, our youth must understand these issues and be informed about best practices. C3 topics and an informed citizenry are also critical in increasing the IT workforce of the future as the Department of Commerce has identified this area as one of tremendous job growth, but predicts there will not be enough graduates in the requisite fields.

Existing Initiatives

Although not including all C3 topics described above, the International Society for Technology in Education (ISTE) has taken a step forward in the creation of its NETS standards. In the summer of 2007, ISTE refreshed their student technology standards. Their website[liv] states**,**

ISTE's National Educational Technology Standards NETS have served as a roadmap for improved teaching and learning by educators throughout the United States. The standards, used in every U.S. state and many countries, are credited with significantly influencing expectations for students and creating a target of excellence relating to technology.

In 2006, ISTE began work on the next generation of NETS for Students,[lv] which focuses more on skills and expertise and less on tools. Specifically, they address:

- *Creativity and Innovation*
- *Communication and Collaboration*
- *Research and Information Fluency*
- *Critical thinking, Problem Solving, and Decision Making*
- *Digital Citizenship*
- *Technology Operations and Concepts*

Digital Citizenship is fifth out of the six listed National Educational Technology Standards for Students (NETS*S). Specifically, ISTE's NETS*S Digital Citizenship addresses how

students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior. To meet these standards, students are to:

a. *advocate and practice safe, legal, and responsible use of information and technology.*
b. *exhibit a positive attitude toward using technology that supports collaboration, learning, and productivity.*
c. *demonstrate personal responsibility for lifelong learning.*
d. *exhibit leadership for digital citizenship.*

ISTE goes further to help guide state and local educational agencies create curricula by detailing a set of general student profiles describing what student behaviors should result from proper instruction in these areas. As ISTE[lvi] (2008) suggests,

The following experiences with technology and digital resources are examples of learning activities in which students might engage during specific grade bands.

The following were suggested for the Digital Citizenship Standard:

PK-Grade 2, (Ages 4-8)

- Demonstrate safe and cooperative use of technology.

Grades 3-5 (Ages 8-11)

- Practice injury prevention by applying a variety of ergonomic strategies when using technology.
- Debate the effect of existing and emerging technologies on individuals, society, and the global community.

Grades 6-8 (Ages 11-14)

- Use collaborative electronic authoring tools to explore common curriculum content from multicultural perspectives with other learners. (2, 3, 4, 5)

Grades 9-12 (Ages 14-18):

- Analyze the capabilities and limitations of current and emerging technology resources and assess their potential to address personal, social, lifelong learning, and career needs. Design a website that meets accessibility requirements.
- Model legal and ethical behaviors when using information and technology by properly selecting, acquiring, and citing resources.
- Create media-rich presentations for other students on the appropriate and ethical use of digital tools and resources.

While one must commend ISTE for developing suggested guidelines, for students, teachers (pre- and in-service), and administrators, it is understood that, in general, state educational organizations (state departments of education and local school districts) operate not necessarily in isolation, but definitely on their own, some adopting ISTE's standards as-is, others creating their own based on ISTE's general outline. While it could be argued that these serve as "guidelines" and other themes and topics could be included,[lvii] the general broad-stroke statements and lack of clarity listed in profiles addressing current topics have resulted in the omission of critical topics in today's curricula. Reinterpretation may be necessary.

Conclusion

The C3 Framework covers a number of critical issues regarding the completeness and quality of Cyberethics, Cybersafety, and Cybersecurity curricula. This policy framework addresses the gamut of C3 issues, and provides examples of the topics to include. The framework is ideal for guiding the practice of the C3 movement nationally, within a region or even internationally. Unfortunately, experiences, literature, and the recent C3 Baseline Survey indicate that most local education agencies do not have policy frameworks on C3 education at all. Where they exist, such policies are limited to interpretations of incomplete standards. AUP policies and student handbook guidelines are presented, but not explained, and as a result, students are told *what not to do*, but may not understand *why*. The C3 framework promotes the teaching of Cyberethics, Cybersafety, and Cybersecurity as a whole. They are pictured as overlapping areas, with both intersecting and interrelated regions, each with a unique focus, but spotlighting the importance of each component. This provides the opportunity for more complete coverage. By spelling out particular elements under each domain, educational entities (Internet safety providers, educational institutions, non-profits etc.) can better design and address critical content and ensure more complete coverage. Teaching C3 issues as one, through branding such as *digital citizenship* or *cyberawareness*, has led to checking off the topic, while missing large swaths of the C3 landscape. Students are described as digitally literate, but have only been informed of a snippet of what should be covered.

The power and possibilities that technology affords students comes with drawbacks if inappropriately used, whether intentionally or unintentionally. Improving student knowledge and awareness of Cyberethics, Cybersafety, and Cybersecurity (C3) concepts will provide them with the means to protect themselves, and will enhance the safety and security of our national infrastructure. Future economic and political stability will be dependent on a safe and secure technology platform, managed by a technologically-savvy workforce.

ENDNOTES

[xlviii] Information on this series can be found at http://www.msnbc.msn.com/id/10912603/

[xlix] http://www.ikeepsafe.org/

[l] http://www.isafe.org/

[li] http://www.netsmartz.org/

[lii] Niels Provos, Anti-Malware Team. Google Online Security Blog. Feb. 11, 2008. All your iframe are point to us. http://googleonlinesecurity.blogspot.com/

[liii] http://www.dhs.gov/xabout/structure/editorial_0839.shtm

[liv] To read more about ISTE National Educational technology Standards see: http://www.iste.org/AM/Template.cfm?Section=NETS

[lv] To read more about ISTE's NETS*S see http://www.iste.org/Content/NavigationMenu/NETS/ForStudents/2007Standards/NETS_for_Students_2007.htm

[lvi] To read more about ISTE's NETS*S see http://www.iste.org/Content/NavigationMenu/NETS/ForStudents/2007Standards/NETS_for_Students_2007.htm

[lvii] Indeed ISTE's publication Digital Citizenship in Schools does touch on a wider interpretation.

Appendix C

Terms and Acronyms

AUP — ***A**cceptable **U**se/Usage **P**olicy* is a set of rules applied to the IT infrastructure of a business, government, educational groups, and website owners, often to reduce the potential for legal action by a user. It is common practice for users of an organization to sign an AUP prior to access to information systems.

C3 — A framework for delivery of ***C**yberethics, **C**ybersafety and **C**ybersecurity* topics in the informal and formal educational setting. Emphasizes the whole, through coverage spotlighting the individual parts to maximize impact and increase citizen awareness of each

IT — ***I**nformation **T**echnology*

LEA — ***L**ocal **E**ducational **A**gency* as defined by the U.S. Department of Education. In simple terms local school districts.

PD — ***P**rofessional **D**evelopment*. Continuing education or training for educators. Can have multiple forms: workshops, in-service trainings, formal classes/courses, conferences, seminars etc.

Appendix D

Focus Group/Interview Protocol

The National C3 (Cyberethics, Cybersafety and Cybersecurity) Baseline Survey provides a means to grab a snapshot of the status of cyber ethics, safety and security education within our nation's schools, and perhaps assist in designing a more comprehensive informal cyberawareness program.

1. How does your state/district/school overall address
    a. Cyberethics,
    b. Cybersafety, and
    c. Cybersecurity in schools (state standards, specific policies, curriculum etc.) for teachers/for students?
        i. What and how are these topics covered (i.e., ethics, plagiarism, copyright etc.)?
        ii. Are these assessed (teachers/students)?
2. What type of C3 Professional Development training is available for teachers (some might not offer—if so reasons, e.g. no funding, other—NCLB emphasis)?
    a. In-service, summits, web-based, courses, conferences
3. Does your state teach C3 topics in the curriculum (separate, stand-alone, integrated)?
    a. If separate, is this due to legislation?
    b. If stand-alone, how (outside presenters—who, how, how often)?
    c. Tell me more about outside presentations (topics covered).
4. Do you anticipate the need for training (for teachers) in the C3 areas?
    a. What C3 issues are of greatest importance?
    b. For education (students), what C3 issues are of greatest importance?
5. What C3 issues do you view as important? Why? (Instances)
6. What C3 issues would you like to learn more about?