National C3 Baseline Study: State of Cyberethics, Safety and Security Awareness in US Schools

Davina Pruitt-Mentle, CyberWatch K12 Division

Abstract: This paper presents the results of the National C3 Baseline Study conducted with 1569 educators and 94 technology coordinators from a web-based instrument. Educators and local education agency (LEA) technology coordinators/directors also responded to an open-ended survey question. Additionally, qualitative data were collected by group and individual interviews. The purpose of the survey was to explore the nature of Cyberethics, Cybersafety and Cyber-security (C3) educational awareness policies, initiatives, curriculum and practices currently taking place in the U.S. public and private K-12 educational settings. Specifically, we were interested in: 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? and What, if any, are the issues and barriers that impede the delivery of C3 content in U.S. K-12 school programs? The results establish base data for C3 awareness program design and provide the foundation for future studies either expanding particular subject areas or examining progress. In addition, results from two 2010 follow on surveys will be shared.

I. Introduction

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)[1] 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. An integrated approach is needed to develop a technologically-savvy needed to operate within the new technology based paradigm. 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 between 75-95% of college students have admitted to academic dishonesty [2]. The Center for Academic Integrity reports that nearly 75% of high school students admit to academic dishonesty. One study conducted in 2000 and 2001, of 4500 students at 25 high schools revealed that 74% admitted to cheating on a major exam [3].The National Crime Prevention Council reports that 43% of teens have been victims of cyberbullying in the last year [4]. Ethical and moral decisions are occurring throughout the students' K-12 experience. The "To Catch a Predator" series on Dateline NBC has highlighted the problem of Internet Predators and the dangers to today's youth. In a 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 and others online [5].

Only recently has Cybersecurity awareness in the educational setting made it to the radar screen. Yet, the Federal Trade Commission (FTC) reports that 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[6]. Key findings from the 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" [7]. 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 listed web browser security, phishing and pharming attachments and unencrypted laptops as just 3 out of 20 top security risks [8]. For 2008, Georgia Tech's Information Security Center's top 5 emerging cyber threats included Web 2.0 and client side

ISBN 1-933510-96-X/$15.00

attacks, targeted messaging attacks, Botnets and threats to mobile convergence and Radio Frequency Identification systems [9]. Google has stepped up its vigilance to report webpages that show up in searches containing malware. Google estimates that more than 1% of all search results contained at least one result that point to malicious content [10]. 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. With the severity of the issues at the national level, and user education listed as a top recommendation, one would assume awareness initiatives would be an important educational goal and be a national priority.

The purpose of the survey was 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, and to establish base data for C3 awareness program design and provide the foundation for future studies either expanding particular subject areas or examining progress. This study used both qualitative and quantitative data. We were particularly interested in:

- 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?

II. METHODOLOGY

This National C3 Baseline Survey gathered and analyzed both qualitative and quantitative data from 1569 public and private U.S. K-12 educators and 94 technology coordinators. This study used descriptive analysis relying extensively on a quantitative Web-based survey 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 emanating 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), and state, regional and local educational organizations, special interest groups, and educational media groups. ETPRO supplied the e-mail 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. All potential participants were informed of the funding source (National Cyber Security Alliance), who was conducting the survey (Educational Technology Policy, Research and Outreach) and 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 missing). 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.

III. 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. The survey data were examined via a variety of statistical methods including means[i], standard deviations[ii], confidence intervals[iii], and other appropriate regression analysis among the variables. Tables and figures are chosen to best represent the data to the reader, 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 [11]. 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 and therefore the survey should have been universally accessible to educators[12]. 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 roles/positions (math teacher, music teacher, media specialist, technology resource teacher, elementary, middle and high school etc.) they played, different geographic location and demographics (state and school size), and differing number of years teaching. Each session lasted between one hour and one hour and 20 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. The survey data were examined via a variety of statistical methods including means[iv], standard deviations[v], confidence intervals[vi], and other appropriate regression analysis among the variables. 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.

IV. KEY FINDINGS

Across the board, this survey found the state of C3 education is limited. Teachers do not feel comfortable with the topics, and standards which set the stage for content coverage, only peripherally discuss the issues. We present here a brief summary listing of survey results and many of the comments made by those we surveyed and those we interviewed.

A. 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 conveying C3 content to students, similar to other content, in the hands of educators. In practice, this responsibility is not necessarily carried out; 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. The coverage of C3 topics included in AUP and student handbooks ranges from 27% up to 73.9%, depending on the topic. 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 to the students.

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 presentations 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.

Schools/school districts do little to promote awareness of Cybersafety and Cybersecurity; they simply eliminate access. Information is conveyed to students on these topics by not allowing any of these opportunities to happen (i.e., downloading is not allowed, students can only go to pre-selected and filtered websites, and/or no email access is allowed). 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 the report, 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.[vii].

Although technology standards have been incorporated within state and local standards, these standards, as reported by survey respondents, include predominantly skills and are often silent on any 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. The respondents captured these thoughts well in their comments.

> *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)
>
> *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)
>
> *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 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)

B. Who's Job is it?

Most C3 instruction has been placed in the hands of the educators, but more than half of the educators do not know how their school informs their students about a variety of issues including protecting, identifying and responding to cyber-crime (i.e, identity theft, predators, cyberbullying, etc.) and how to identify signs of documents and emails containing viruses. However, many educators do not feel that C3 topics should be their job; they feel it should be covered by parents. This may be possible in some households, but many parents lack the skills to inform their children about online safety and computer security. This is particularly problematic in children who are immigrants, or children of immigrants whose parents have a limited educational background, and often no technology knowledge. 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. The school administration is often reluctant to face such conflicts, and in many cases fail to support their teachers.

> *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)

C. 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. In Cybersecurity, 67% of educators 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.

> *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)
>
> *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)

D. 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 6 hours of professional development on C3 topics in the last 12 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.

> *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)
>
> *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)
>
> *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)

E. Concern, Need and Want

This baseline survey was not an inconsequential survey. It was extensive and took a non-trivial 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 survey compelling enough to participate in focus groups for the survey. Clearly with all the demands on educators, this fact alone can indicate 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. I hope to hear more about your study and program.* (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)

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)

I hope we participants will get to see the results of this survey. (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)

V. 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 and integration techniques. Over the course of the years, and especially more recently, the emphases have been on technology integration in the classroom and thus providing students hands on opportunities to use technology. Although this level of integration varies from classroom to classroom on a national scale, the fact remains, the focus has still been on *instructional use* with *Cyberethics, Cybersafety and Cybersecurity (C3) issues* taking a back seat, in spite of the fact that these issues are playing center stage in today's 21st century world. 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 (or using the general term Internet safety), cyberbullying, schools expanding their Acceptable Use Policies (AUP), PTA safety assemblies, and a plethora of Internet safety providers engaged in awareness campaigns and speaking engagements. 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.

This report provides valuable information into how and through what efforts state, regional and local institutions are addressing C3 awareness while under the financial constraints, time commitments, bureaucratic processes, and an already over packed curriculum agenda that make it difficult for schools to successfully pursue C3 awareness efforts at the level they believe is necessary to meet the needs of their students and educators.

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 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 interesting in learning more about C3 topics, and that Cyberethics, Cybersafety and Cybersecurity are important and critical components to using technology appropriately. Overall, 53.8% of educators feel 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 under the domains-particular safety and security, and include program evaluation. More hands-on training opportunities for educators (not just resources and assemblies), and increased and on-going opportunities for youth throughout the K-12 experience would provide the comprehensive effort needed to close the gap between danger and knowledge.

It should also be noted, the knowledge limitations of both educator and student affects their ability to protect the local education agency IT infrastructure, and may serve as a potential danger to their own information based on their limited consumer awareness.

ISBN 1-933510-96-X/$15.00

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 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 which were conducted for this survey, and personal experience gained over the past fifteen years on these topics, we believe our 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 upwelling 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.

VI. 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. Although, as a result of today's funding constraints and full curricula, this is understandable; it should be done with caution. Only via a concerted and united effort can we keep both our children and our national IT infrastructure safe and secure.

A. 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)

Cyberethics, Cybersafety and Cybersecurity are not ideas whose place is only within the educational domain. They cut across education, government and industry and are imperative to both our success and our security in the 21st Century. All three need to be included in a national initiative program. 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. Business and industry driving technology advancement may be most able to provide the expertise in some areas, for example, 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 covered.

Impact requires a thrust using multiple means. Current efforts serve as only a band aid as most instruction is either reading 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 content coverage, whether in the classroom or an at one time workshop for teachers has little impact. Ongoing content instruction is needed throughout the K-12 experience; starting early (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 continual presentation of material and lessons to students. Training is also needed for both parents and educators who can pass the information on to their students/children, and can reap the benefits of this training for themselves.

In addition to content in the classrooms, and teacher training, a national campaign needs to take place, similar to recent awareness campaigns for green energy technologies and obesity. Public service announcements, talk shows and morning 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 cyberethical, safe and secure technology use. The possibilities are endless. But one thing is sure, success can only result from a multi-means effort which includes a variety of partners focused on the common goal – protecting our children and our nation, and preparing for tomorrow.

B. C3 Framework

Schools tend to pick and choose which C3 topics to teach, and often only talk about Cyberethics, i.e. 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

ISBN 1-933510-96-X/$15.00

taught as a whole, yet each has a unique focus, spotlighting their components' importance, provides the opportunity for more complete coverage. Although we understand that 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 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.

C. 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, and many of the current concerns (cyberbullying through text messages, cell phones cameras to send test questions to friends, identify theft through social networking sites and malware through media rich plug ins) did not even exist. While standards are often broad based to allow flexibility to new and current growing concerns, they need to be interpreted beyond the broad stroke basics to make an impact. Perhaps, areas such as technology require more frequent refreshing or at minimum, additional content examples via a yearly update to keep pace with change.

D. Comprehensive, Systemic and Sequential Content Suggested

We do not assume that topics such as fractions can be taught in a day. In fact, not only is it considered a multi-day unit, students are re-exposed to the content over several years as appropriate to their learning level. Yet, complex topics such as those encapsulated within Cyberethics, Cybersafety and Cybersecurity, which admittedly are not understood by educator respondents in this survey, are covered in a single session. We know from decades of research that presenting material multiple times; in multiple ways, sequentially over time has the best return and maximum impact. 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.

E. Professional Development for Teachers a Must

Just because a topic area is listed in a standard does not mean teachers are prepared to inform students on the topic. Educators see the need, want to learn more and are willing to put in the effort to learn these 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. We continue to place new demands on our teachers, yet professional development opportunities on some of these content areas are limited. Teachers need training. Many school systems do not have the expertise and the majority lacks the funding to deliver professional development 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 to both 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 training is almost non existent. If indeed national security, economic welfare of citizens, safety for youth and a needed nudge for more ethical behavior across U.S. society is desired, then government, business/industry, and education need to team up to provide the needed information to our teachers.

F. Don't Forget Informal Settings

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 are an important means to yield additional learning opportunities which impact today's youth. These potential content providers should not be ignored, and should be used as additional intervention opportunities. However, similarly as with teachers, leaders (both volunteer and professional) need instruction in C3 topics, and can benefit from pre-made learning units for their group. Once again, members of the business community can be leveraged to provide expertise which can enhance presentations with real-world experience, lessons, and opportunities.

Some teachers feel that C3 education is the responsibility of parents. However, many are not prepared with the tools to deliver information in these areas. Some students are the children of immigrants without technology knowledge, and others may be in alternative homes (i.e., foster care or are without legal guardians), which do not

ISBN 1-933510-96-X/$15.00

have the wherewithal to deliver C3 information. Many adults have only limited computer literacy skills and or language skills. If educators do not deliver the information, informal settings may be the only place for children to receive the content.

G. Policies: Beyond Printed Text

The pace of change of technology requires continual updates to content and standards. The technology portions of AUP 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 employees (including teachers), students and parents understand them. The topics need to be covered more 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 covered in on-going instruction, especially to ensure new transfers receive the information. It is imperative that consequences are included and supported by administrators and school authorities (school boards and superintendent). Teachers currently feel unsupported and let ethical violations go rather than follow ill-defined and unenforced policies.

H. 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 IT department, and ignore the topics both in the classroom, and in their personal behavior. For example, they assume all information on the school network is secure. However, security is only as strong as the weakest link. Educators may not use best practices to protect the IT infrastructure, i.e., they use weak passwords, they add unapproved software to their computers, and allow others to use their computers. They also lose 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 gives a false sense of security and unrealistic expectation. We need to make sure teachers understand their role in all C3 areas. Local education agencies need to change their focus from Cybersecurity and Cybersafety being limited to filtering, blocking and policies that say no blogs or social networks, to more individual responsibility and understanding on how to use technology wisely. When students leave school they need to know what is appropriate and effective so they are prepared for IT environments with less protection and can act responsibly.

I. 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 efforts being offered in schools. Improving learning includes understanding knowledge gaps, providing instruction, evaluating impact, and redesigning instruction. This process is aided by the use of best practices, peer evaluation, and innovation which can only be accomplished through moving forward rather than reinventing the same content in different schools. Additionally, existing content can be used as a form of professional development for teachers prior to their use of the curriculum in the classroom. By understanding what content is used in the classroom, we can understand not only whether this content is making an impact, but we can also understand why there are knowledge gaps, indicated by a lack of existing lessons.

VII. REFERENCES

[1] Pruitt-Mentle, D. (2000). The C3 framework: Cyberethics, Cybersafety and Cybersecurity Implications for the Educational Setting. *Proc. 2000 MICCA Conference.* May 2000, Baltimore, Maryland.

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

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

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

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

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

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

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

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

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

[11] 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

[12] NCES: Internet Access in U.S. Public Schools and Classrooms. http://nces.ed.gov/surveys/frss/publications/2005015/index.asp?sectionID=2

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

---

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

[ii] 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

[iii] 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.

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

[v] 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

[vi] 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.