ETPRO – NCSA

Extracted from:

2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study

October 2008

Full Report Available from:
http://staysafeonline.mediaroom.com/index.php?s=67&item=44.13

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

for

National Cyber Security Alliance
www.staysafeonline.org

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.

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 partici-

pating 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 respon-

dents 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 set-

tings 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 Information 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

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, often school policies and instruction are uncoordinated and do not include all Cyberethics, Cybersafety, and Cybersecurity (C3®) topics because state and local education agency standards use broad-stroke statements to guide curriculum and competency. Interpretations of these standards or guidelines have in some cases missed the mark related to C3 issues and how they correlate with human behavior. Ethics is intended to represent personal choice. Using the analogy of riding a bicycle, ethically we choose not to ride on our neighbors grass. Safety refers to safe practices, i.e. ride on the right side of the road, and obey traffic laws. Security refers to additional items we have to do, for example adjust gears and brakes. The first is a moral choice, the second is the way we behave, and the third requires further action, and each operates at a different cognitive level and therefore needs to be taught differently. Clearly there is overlap between each, however the differences are important to address.

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." Analogously, automobile education is not one amorphous topic, but includes topics such as road rage (ethics), keeping tires inflated and following laws (safety), and alarms (security). 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 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
- Online gambling
- Gaming
- Internet addiction

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*[xi] 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 iKeep-

Safe,[xii] iSafe,[xiii] and NetSmartz.[xiv] 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[xv]. 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[xvi] 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[xvii] 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,[xviii] 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[xix] (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,[xx] 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.

ENDNOTE

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

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

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

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

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

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

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

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

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

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