Testimony and Statement for the Record

Rodney J. Petersen
Policy Analyst and Security Task Force Coordinator
EDUCAUSE

Hearing on
"Protecting Our Nation's Cyber Space:
Educational Awareness for the Cyber Citizen"

Before the
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
Committee on Government Reform
United States House of Representatives

April 21, 2004
2154 Rayburn House Office Building

Mr. Chairman and members of the committee, thank you for the opportunity to testify today regarding education and awareness for the cyber citizen. Educational institutions, from kindergarten through college, are familiar with the importance of education and are actively preparing citizens who will contribute to the information economy. I am especially pleased that by holding this hearing you recognize the importance of education and awareness as part of an overall strategy to improve the cyber security of our Nation. The present challenges of cyber security require the establishment of a life-long culture of security from the cradle to the grave.

I must stress at the outset, however, that education and awareness will not be enough. The driver of an automobile must understand the rules of the road and be trained to drive safely. However, if the car is not manufactured for safety or the road is not appropriately engineered and professionally maintained, no amount of driver safety education will prevent accidents. Similarly, education and awareness are a necessary but insufficient approach to protecting our nation's cyberspace. I believe that the series of hearings that you held during the fall and the subsequent work of the Corporate Information Security Working Group appropriately recognizes that cyber security is a multifaceted problem requiring diverse and complementary solutions.

EDUCAUSE and Internet2

I am here today on behalf of the EDUCAUSE/Internet2 Computer and Network Security Task Force <www.educause.edu/security/task-force.asp>.

EDUCAUSE <www.educause.edu> is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. The current membership comprises nearly 1,900 colleges, universities, and education organizations, including more than 170 corporations. EDUCAUSE has offices in Boulder, Colorado, and Washington, D.C.

Internet2 <www.internet2.edu> develops and deploys advanced network applications and technologies for research and higher education, accelerating the creation of tomorrow's Internet. Led by more than 200 U.S. universities and working with industry and government, Internet2 recreates the partnerships among academia, industry, and government that helped foster today's Internet in its infancy.

Computer and Network Security Task Force

EDUCAUSE and Internet2 established the Computer and Network Security Task Force in July 2000. The Task Force is working to improve awareness among the EDUCAUSE and Internet2 memberships and throughout higher education. The Security Task Force actively promotes effective practices and solutions for the protection of information assets and critical infrastructures. The Security Task Force is coordinating its efforts on behalf of institutions of higher education with the support of the Higher Education Information Technology Alliance <www.heitalliance.org> whose members include the American Council on Education, Association of American Universities, National Association of State Universities and Land-Grant Colleges, American Association of State Colleges and Universities, National Association of Independent Colleges and Universities, and the American Association of Community Colleges.

National Strategy to Secure Cyberspace

The Security Task Force prepared the *Higher Education Contribution to the National Strategy to Secure Cyberspace*. The *National Strategy* encourages colleges and universities to secure their cyber systems by establishing some or all of the following as appropriate:

- one or more Information Sharing and Analysis Centers to deal with cyber attacks and vulnerabilities;
- an on-call point of contact to Internet service providers and law enforcement officials in the event that the school's IT systems are discovered to be launching cyber attacks;
- model guidelines empowering chief information officers to address cyber security;
- one or more sets of best practices for IT security; and,
- model user awareness programs and materials.

The Security Task Force was also well represented at the recent National Cyber Security Summit and participated on each of the five task forces. I was a member of the Task Force on Awareness for Home Users and Small Businesses. The scope of the task force was expanded to include large enterprises and state and local government, as well as schools and institutions of higher education. I served as the co-chair for the Subcommittee on Schools and Institutions of Higher Education. Therefore, my testimony today will address education and awareness from kindergarten through college based upon the findings and recommendations of the subcommittee.

Elementary and Secondary Schools

Colleges and universities have long been interested in supporting the efforts of elementary and secondary schools to improve the awareness of students on issues such as cyber ethics and security. After all, life-long habits are formed early—the better we educate students about online safety in the K–12 setting, the less we will need to do so when they arrive at college. Similarly, cyber security awareness facilitated by schools will benefit companies and government agencies that will eventually employ a new generation of technology-savvy and security-conscious workers.

There is a legion—54 million strong—of young people who can lead the nation in secure and trustworthy computing. Many will enter a high-tech-enabled workforce during this decade. The U.S. Department of Education counts 53.8 million children (K–12) in our nation's public and private schools. Together, these students have at least 75 million parents or household caregivers. A systematic program for teaching secure and trustworthy computing skills K–12, therefore, has the opportunity to "trickle up" and reach at least 125 million people. This is nearly the number of Americans—146 million—who currently use the Internet. Because of this trickle-up phenomenon, investment in cyber security education and Internet-skills training will begin to pay off immediately.

Our current notion of cyber security must start in kindergarten

In the past, cyber security has been the domain of computing professionals and law enforcement agencies. But with the mainstreaming of the Internet, cyber security is now a shared responsibility of adults and tech-savvy children alike.

At this juncture, young people must be taught effective cyber skills from the moment they are first allowed to touch a computer mouse. As soon as children enter kindergarten, they are capable of embracing age-appropriate, responsible computing practices. Their parents and older siblings will be challenged to catch up with them.

Developing good habits young is essential to building a positive culture of cyber security

Once habits are formed, they are difficult to break regardless of age. Whether the habit is weight control, fingernail biting, or poor information security practices, it is better to mold positive behavior than to modify negative behavior. Research in youth crime prevention suggests that intervention with at-risk children at a very young age curbs the onset of

delinquent behavior by up to 80 percent. Hence, it's reasonable to infer that positive cyber skills must be introduced at the youngest possible age. For adults, this means making it more convenient and easier to "do the right thing" and making each adult an individual stakeholder in the practice of secure cyberspace habits.

Project NEThics at the University of Maryland

While at the University of Maryland, I was the founder of Project NEThics <www.umd.edu/NEThics>—a group dedicated to the promotion of legal and ethical use of computing resources. Every spring, the University hosts Maryland Day, inviting members of the local community onto the College Park campus for family fun and educational activities. One year, Project NEThics in partnership with the Prince George's County Computer Forensics Unit set up a computer lab where we invited children along with their parents to participate in activities designed to increase the awareness of children for online safety. We also talked with parents to encourage adult supervision of their children's online activities and to acquaint them with the benefits and risks of networked computer use. We provided literature to parents, including an online safety pledge provided by the Center for Missing and Exploited Children.

Project NEThics also collaborates with the College of Education to develop seminars for teachers and school media specialists on cyber ethics and security. This summer, the university will host a conference entitled "Cyberethics, Cybersafety, and Cybersecurity for Professional Educators" <www.edtechoutreach.umd.edu/cyberethicsseminar2004.html>. The conference will address implications for classroom and higher education technology instruction. The program flyer notes:

> Unfortunately, while the teaching of technology processes and skills has been handed to the classroom teacher, most educators lack the knowledge and up-to-date information related to security issues. Teachers, in many instances, model incorrect protocol and behavior to their students. Not only does this increase the risks to the security of the teacher's own classroom and local school system's information systems, but it also increases the chances that students will follow their behaviors.

Consortium on School Networking (COSN)

COSN <www.cosn.org> is a national non-profit organization whose mission is to advance the K-12 education community's capacity to effectively use technology to improve learning through advocacy, policy and leadership development. COSN members represent school districts, state and local education agencies, nonprofits, companies and individuals who share the organization's vision.

COSN, in partnership with Mass Networks Education Partnership (Mass Networks), is developing a program – Cyber Security for the Digital District - to provide schools and school districts with vital information on education networks in order to ensure the privacy and the security of data within their systems. The three-year project combines both government and private sector support to help the superintendents and chief technology officers of local school districts better understand how to deal with cyber security. COSN is creating materials to raise awareness of school administrators and to help them raise the awareness of their community. COSN is creating tools that K–12 leaders can use, developing a Web site for dissemination and sharing of information, and planning training workshops and other activities. More information about the project, Cyber Security for the Digital District, is available at securedistrict.cosn.org.

CyberSmart!

CyberSmart! <www.cybersmart.org> provides K-12 curricula and training programs teaching secure, responsible, and effective computer and Internet use. The CyberSmart! K–8 Curriculum is a free "owner's manual" for students' safe, responsible, and effective use of computers and the Internet. It complements all academic subjects, emphasizing character building and skill-based decision making related to successful technology use.

Developed by professional educators, curriculum experts, and Internet industry innovators, the CyberSmart! Curriculum meets the needs of school administrators, teachers and students by

- enabling schools to successfully execute technology plans;
- addressing the social, legal, and ethical issues associated with technology use;
- supporting teachers in their efforts to successfully integrate technology into the classroom;
- providing students with the tools they need to navigate the Internet safely, sensibly, and effectively; and,
- involving families.

CyberSmart! proposes the following action agenda for securing the nation's digital resources:

- Federal, state, and local governments must participate in funding for cyber security education programs, particularly those involving America's 50 million K–12 students.

- Industry, government, and other interested parties must engage in coordinated public awareness campaigns that stress the value of individuals—both adults and young people—to communicate and share information responsibly and securely online.

- The core group of industry trade associations and nonprofits involved with promoting Internet education must expand. Now is the time to reach out to outlying trade groups to enlist broad-based industry support for cyber security education. Organizations representing securities, banking, health care, media, education, and other industries all have significant roles to play.

- The high-tech industry must implement practical cyber security technologies that combine ease-of-use convenience, low cost to widespread deployment, and respect for privacy.

- Both the private sector and government should engage in research to determine the best information security educational practices.

- Schools must teach secure, responsible computing skills as part of a mandated component of K–12 curriculum nationwide.

- The U.S. Department of Education and states must prioritize teacher training for cyber skills, including information security skills, in order to effectively leverage technology in support of student achievement and to prepare students to enter the technology-enabled workforce.

- The benefits associated with teacher training must be communicated to the senior education administrators who allocate and administer funds.

- The essential role of librarians as highly skilled navigators of an increasingly complex web of data sources must be acknowledged and support provided to librarians—in schools, universities, and public and private settings—to strengthen the use of the Internet to sustain the integrity of academic achievement, life-long learning, and the democratic processes.

Colleges and Universities

The EDUCAUSE/Internet2 Computer and Network Security Task Force received a grant from National Science Foundation to identify and implement a coordinated strategy for computer and network security for higher education. The following strategic goals have been identified:

- **Education and Awareness.** To increase the awareness of the associated risks of computer and network use and the corresponding responsibilities of higher education executives and end users of technology (faculty, staff, and students), and to further the professional development of information technology staff.

- **Standards, Policies, and Procedures.** To develop information technology standards, policies, and procedures that are appropriate, enforceable, and effective within the higher education community.

- **Security Architecture and Tools.** To design, develop, and deploy infrastructures, systems, and services that incorporate security as a priority; and to employ technology to monitor resources and minimize adverse consequences of security incidents.

- **Organization and Information Sharing.** To create the capacity for a college or university to effectively deploy a comprehensive security architecture (people, process, and technology) and to leverage the collective wisdom and expertise of the higher education community.

<u>Security Task Force Education and Awareness Working Group</u>

The Security Task Force has created an Education and Awareness Working Group to identify and take steps to implement and publicize various methods by which awareness of information technology security issues are raised among university and college computer and network users, administrators, and executives. The working group has identified categories of audiences for which to target education and awareness:

- **Executives:** The first item in the "Framework for Action" developed by the Security Task Force in 2002 was to "make IT security a higher and more visible priority in higher education." As reported in the Corporate Governance Task Force report issued earlier last week, chief executives and governing boards must assume direct responsibility for securing their computer networks.

- **All Users:** Raising the consciousness of the end users of networked computers is a goal higher education holds in common with government and industry. The EDUCAUSE/Internet2 Security Task Force is proud to affiliate with the National Cyber Security Alliance to assist them in the development of a broad national campaign for home users. A baseline of information is needed by everyone, and we are striving to keep messages consistent across groups that are developing awareness materials. It is important here to acknowledge the National Cyber Security for providing content from the Alliance's whitepaper "An Action Agenda for Security the Nation's Digital Resources: Start in Kindergarten!" (April, 2004), which has been integrated within this document.

- **Members of Information Assurance (IA) Teams:** Information security is no longer just the concern of the IT security officer. Auditors, risk managers, legal counsel, business officers, police and public safety officers, chief information officers, data stewards, and chief security officers play critical roles in an enterprise information security program. The training and professional development needs of IA team members are significant and must be supported on an ongoing basis.

- **Users of Business Systems:** Certain individuals are granted privileges to access critical systems that contain sensitive data. In higher education, administrative computer systems typically contain data related to personnel, student information and education records, grants and contracts, financial information, and other confidential or proprietary information. Special care must be taken to safeguard confidential information and records.

- **Information Technology Staff:** A skilled IT workforce is critical to efforts to protect information assets and critical infrastructures. Employees responsible for system administration, network operations, database administration, Web development, and applications development require continual training and professional development to keep up with the growing demands for security. Help desk personnel must also understand cyber security best practices so they can effectively convey security awareness messages to end users.

- **Faculty, Staff, Students, and Guests:** Individuals interact with technology differently depending on their specific roles or responsibilities within a college or university. Educational levels as well as cultural influences may vary among audiences. Therefore, education

and awareness should be customized to address target populations in academic or residential settings.

Campus security awareness efforts

A number of campuses have instituted cyber security awareness programs. Techniques range from distributing note cards and flyers and displaying posters to video performances, skits, presentations and seminars, and letters from campus officials. Increasingly, efforts are made to convey important security and policy information to students at the time of new student orientation. In a few cases, institutions have implemented online quizzes or mandatory information sessions as a condition for obtaining access to the campus network.

A listing of college and university security awareness initiatives is available at www.educause.edu/security/resources/awareness.asp.

Cyber Security Day

Colleges and universities across the country recently planned security education and awareness events between March 29 and April 2, 2004, to help promote Cyber Security Day (April 4, 2004). The Security Task Force fulfilled one of the recommendations of the Awareness Task Force report by encouraging and supporting events at higher education institutions that observe Cyber Security Day (see the appendix). The Education and Awareness Working Group of the Security Task Force is building momentum toward the next Cyber Security Day on October 31, 2004. We expect a number of campuses to plan activities during the week prior to the day or throughout the month of October.

National Information Assurance Training and Education Center (NIATEC)

NIATEC <www.niatec.info> is a consortium of academic, industry, and government organizations developed to improve awareness, training, and education standards in Information Assurance. It is the federally designated cornerstone for essential education and training components of a strong Information Assurance initiative. The NIATEC is associated with Idaho State University Center of Academic Excellence. The Centers of Academic Excellence and NIATEC are components of a plan to establish a federal cyber corps to defend against cyber-based disruption and attacks. The national plan proposes to address the increasing vulnerability to such attacks; emphasizes the role of academia in cyber defense; and calls for active partnerships among private sector, academia, and governmental organizations. Key to building such a cyber corps is the implementation of robust graduate and undergraduate curricula in Information Assurance.

Conclusion

Tremendous progress has been achieved but much work remains to be done. First, if the improvement of cyber security is indeed a national priority, as we think it should be, then we need to see an infusion of public and private support flowing to our schools and institutions of higher education.

Second, the baseline information required by all users of networked computers to operate safely online must be kept to a minimum to accommodate a diverse range of learning styles and educational levels.

Third, there should be consistency in basic awareness messages whether presented to kids in schools, adults in college, employees in the workplace, or home users. The messages should be simple, straightforward, and easy to understand.

Finally, efforts to increase awareness and education regarding cyber security and ethics must happen in parallel to the development of more-secure technologies.

Schools and institutions of higher education must also develop more-secure technical architectures and provide security-related services, and the IT vendor community must strive to improve the security of hardware and software widely used in open, collaborative educational environments.

Appendix

FOR IMMEDIATE RELEASE

Contacts:
Rodney Petersen
Policy Analyst and Security Task Force Coordinator
EDUCAUSE
rpetersen@educause.edu
202-331-5368

Michelle Pollak
Media Relations Manager
Internet2
mpollak@internet2.edu
202-331-5345

****
COLLEGES AND UNIVERSITIES RECOGNIZE CYBER SECURITY DAY WITH CAMPUS EVENTS
****

Washington, D.C., March 26, 2004—Setting your clocks forward or back for daylight saving time and replacing the batteries in smoke detectors are rituals repeated every spring and fall. Similarly, the National Cyber Security Alliance (<http://www.staysafeonline.info>) established April 4, 2004, as Cyber Security Day to raise awareness about Internet safety and computer security issues. Colleges and universities across the country are planning security education and awareness events between March 29 and April 2 to help promote Cyber Security Day.

Rutgers University is encouraging its students, faculty, and staff to "Spring Ahead to Security!!" on a Web site devoted to National Cyber Security Day (<http://rusecure.rutgers.edu/cybersecurityday/>). In addition to campus presentations on identity theft, the Web site suggests steps that the campus community can take "in the quest for better security" such as using antivirus software and keeping it up-to-date weekly, exercising caution when opening e-mail attachments, selecting hard-to-guess passwords and keeping them private, backing up important files, downloading and installing operating system update patches, avoiding risks of file sharing, using a password-protected screensaver, locking up computers when not in use, and using a firewall to protect computers from intruders. Lance D. Jordan, director of Information Protection and Security at Rutgers, said, "Providing personal information over the Internet has become a risky proposition, and our

community needs to be aware of the risks and protective measures that are easily practiced to surf cyberspace safely."

The George Mason University IT Security Office is featuring a week-long lineup of lunchtime presentations promoting cyber security awareness (<http://security.gmu.edu/nationalcybersecurityday.html>). Topics include network security and denial-of-service attacks, desktop strategies to secure your cyberspace, file sharing, and more. Joy Hughes, CIO and vice president for Information Technology at George Mason, believes that it is important for faculty, staff, and students to have a role in planning security awareness events. She said, "Our workshop content is determined by consulting with the members of the university-wide Systems Administrators' Leadership Team; the Security Review Panel; and other faculty, staff, and student groups working to improve security."

The University of Arizona developed a series of humorous posters to reinforce messages that are designed to prevent identity theft and other consequences of improperly secured computers (<http://security.arizona.edu/posters.html>). The slogan for the Arizona campaign emphasizes that the key to security is derived from the word itself: sec-U-R-IT-y. In other words, "You Are It!" Kelley Bogart, an analyst in the Information Security Office at the University of Arizona, is co-chair of the Education and Awareness Working Group of the EDUCAUSE/Internet2 Computer and Network Security Task Force that is encouraging higher education institutions to hold events in conjunction with Cyber Security Day. "We want information technology users to understand that they are part of the solution. Although good security should be practiced every day throughout the year, we believe there is benefit in colleges and universities participating in a national campaign that focuses everyone's attention on the critical problems associated with information security," Bogart said.

Shirley Payne, director of Security Coordination and Policy in the Office of Information Technologies at the University of Virginia and a member of the Security Task Force Education and Awareness Working Group, remarked, "Think of this scenario: The CEO of a major corporation is hearing about cyber security at work. When she gets home, her young son shows her a poster he's crafted to submit to a cyber security poster contest. Turning on the TV, she sees a public service announcement concerning the need to secure her home computer, and driving to work the next day, she hears an NPR interview on the great successes of higher education in reducing the impact of viruses and worms." Payne has published on the topic of developing campus-wide security education and awareness in *EDUCAUSE Quarterly* ([PDF 57 KB]

<http://www.educause.edu/ir/library/pdf/EQM0347.pdf>) and in a new book entitled "Computer and Network Security in Higher Education." The University of Virginia is also part of the Virginia Alliance for Secure Computing and Networking (VASCAN) that has compiled a collection of security tools and best practices from Virginia universities (<http://www.vascan.org/categories/security_awareness.html>).

The EDUCAUSE/Internet2 Security Task Force is a sponsor of the National Cyber Security Alliance and supports efforts to promote online safety and create security awareness among the general public. The Security Task Force also contributed to the Awareness and Outreach Task Force report released on March 18 by the National Cyber Security Partnership (<http://www.cyberpartnership.org/>). The Security Task Force is fulfilling one of the recommendations of the report by encouraging and supporting events at higher education institutions that observe Cyber Security Day. The next Cyber Security Day will be on October 31, 2004.

****

ABOUT EDUCAUSE

EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. The current membership comprises nearly 1,900 colleges, universities, and education organizations, including more than 170 corporations. EDUCAUSE has offices in Boulder, Colorado, and Washington, D.C. Learn more about EDUCAUSE at <http://www.educause.edu/about/>.

ABOUT INTERNET2

Led by more than 200 U.S. universities, working with industry and government, Internet2 develops and deploys advanced network applications and technologies for research and higher education, accelerating the creation of tomorrow's Internet. Internet2 recreates the partnerships among academia, industry, and government that helped foster today's Internet in its infancy. For more information about Internet2, see <http://www.internet2.edu>.