

STARLINK®

An Agency of the Texas Association
of Community Colleges

presents

CYBERINSECURITY:

PREVENTION AND PROTECTION SOLUTIONS

PARTICIPANT PACKET



Produced by:
Dallas Teleconferences



In cooperation with:
American Association
of Community Colleges

APRIL 8, 2004
1:30 - 3:00 PM CT



Presented by:
PBS-Adult Learning Service



“CYBER INSECURITY: Prevention and Protection Solutions”

Agenda	3
Participating by Telephone, FAX, E-Mail	4
Fax-In Question Sheet	5
About the Panelists and the Moderator	6
Articles:	
“The Growing Vulnerability of Campus Networks”	8
“Scale the Solution to the Problem”	14
“A(n Extended) Campus Information Security Conversation”	20
Local Activities	23
Resources	24
Upcoming Events from STARLINK	28
Videotape Order Form	29
Evaluation Form	30

You have permission to duplicate print material in conjunction with this videoconference only.



“CYBER INSECURITY: Prevention and Protection Solutions”

Opening Credits	2:30 pm <i>(all times Eastern)</i>
Introduction	2:31 pm
Videotaped Scenarios on Cybersecurity Issues	2:35 pm
Scenario #1, #2, and #3	
Analysis and Discussion by Moderator and Panelists	
Q and A with Audience	2:52 pm
Email and Fax Questions	
Videotaped Scenarios on Cybersecurity Issues	3:00 pm
Scenario #4, #5 and #6	
Analysis and Discussion by Moderator and Panelists	
Q and A with Audience	3:17 pm
Email and Fax Questions	
Videotaped Scenarios on Cybersecurity Issues	3:25 pm
Scenario #7, #8, #9 and #10	
Analysis and Discussion by Moderator and Panelists	
Q and A with Audience	3:42 pm
Telephone, Email and Fax Questions	
Program Summary	3:55 pm
Program End	3:58 pm

**Subject to change.*

PARTICIPATING BY TELEPHONE, FAX AND E-MAIL



YOU can be a participant, not just a passive viewer, in this videoconference by interacting with the panelists in the studio. Your participation will enrich the videoconference for you and for others throughout the nation who have similar concerns and interests.

There are three ways to interact with the presenter: Call-in, Fax, and E-Mail.

CALL IN: The toll-free telephone number for call-in questions is: 1-800-745-0371.
(If the line is busy when you call, please try again.)

How It Works: Your call will be answered by a member of our staff, who will ask for your name and site location. You will then be put on hold. While you are on hold, you will be able to hear the videoconference through the telephone. Stay on the line so we can communicate with you if necessary. If your call should be accidentally disconnected, call again and tell the operator you were disconnected while waiting to ask a question.

Calls will be put on the air "live." When prompted or introduced by the program host, give your name and site location, and state your question(s) as clearly and succinctly as you can. Please be aware that while you are asking your question, you will be "on the air."

Avoid Confusion: There most likely will be a time delay between what you hear over the telephone and what you may hear over the audio speakers at your site. This is normal, and you should concentrate on and be guided by what you hear over the telephone. Ignore what you might hear over the audio speakers at your site.

Better Audio: To minimize the possibility of any technical or program difficulties that may be caused by audio feedback, we suggest you locate the telephone away from the audio speaker at your site.

FAX: Use the sheet on the following page to send your question or comment ANY TIME from now until the end of the videoconference at 4:00 p.m. ET on the day of the live event. The sooner we receive messages via FAX, the better we can respond effectively. Use the Fax-in Question Sheet provided on the next page.

Please use the fax-in form provided on the next page.

Before April 8: (972) 669-6699

On April 8: (972) 669-6633

**EMAIL: Send questions or comments for the panelists to
Teleconferences@dcccd.edu – PLEASE put “CyberInsecurity” in the subject line.**

FAX-IN QUESTION SHEET



Write your question in the space provided below.
Please limit it to a maximum length of 25 words and print clearly and legibly.

A large rectangular box with a black border, containing 15 horizontal lines for writing a question.

Name (optional): _____

Institution/State (optional): _____

E-mail (optional): _____



Panelists:

PAUL HARRIS, CISSP, Security+, Director IT Security Education for St. Petersburg College (SPC) in Florida. He came to the college after a career in law enforcement, where his duties included investigating computer-related crimes. He served as a police officer and a detective, as well as an administrator with the Florida Department of Law Enforcement. As an educator, he researches and develops new technology programs. He led the project for SPC to become the first “(ISC)² Authorized Academic Center” in the world and is now administrator of the academic center program for other colleges, in partnership with (ISC)². Paul has developed education programs for computer-related crime investigations, IT Security, Secure Coding, Project Management, and Quality Assurance. These programs are shared with other colleges who want to develop their own education programs in these topics. In addition he has also consulted on cybersecurity issues with members of Congress, the executive branch of the federal government, business and law enforcement agencies. Additional projects include hosting the annual “Cyber Security Summit” with the FBI at SPC, SME for the CompTIA Security+ certification, SME for the governor’s Digital Divide committee, board member of the “Internal Controls Institute”, former board member of United Way and speaking at national conferences. Paul’s standard question for IT staff and administrators in higher education is “How well does your institution’s CIO sleep at night?”

RANDY MARCHANY has been involved in the computer industry since 1972. Randy is currently the senior member of the VA Tech Computing Center’s Unix system management group. He is the director of the Network Appliance Testing Laboratory, which is part of VA Tech’s CIRT and Network Defense Initiative and the coordinator of VA-CIRT, an incident response team made up IT staff from various state universities in Virginia. He is the author of VA Tech’s “Acceptable Use Statement,” which has become a model for the Virginia state university system. He has been a frequent speaker at national and international conferences such as SANS, IIA, ISACA, Network Security, IEEE Symposium on Systems Management, DECUS, and the Computer Security Conference. The SANS Institute has described him as the “best storyteller in the computer security field.” He has taught professional development seminars on Unix System Management, Forming Incident Response Teams, Auditing Unix Systems, Auditing Internet Security for various professional groups such as ISACA, IIA, Ernst & Young and the SANS Institute. He is co-author of the SANS Institute’s “Top 20 Internet Security Vulnerabilities” document that has become a standard for most computer security and auditing software. He is also a co-author of the SANS Institute’s “Computer Security-Incident Handling-Step by Step” which has been recognized as one of the foremost publications on Incident Response. He was a recipient of the SANS Institute’s Security Technology Leadership Award for 2000. Randy holds a B. S. in Computer Science and an M. S. E. E. from Virginia Polytechnic Institute and State University. He is a member of the award-winning string band No Strings Attached, participates in several sports including volleyball, handball and biking, and was an assistant volleyball coach for VA Tech’s women’s volleyball team.



DANIEL A. UPDEGROVE is Vice President for Information Technology at The University of Texas at Austin, and senior lecturer in the UT Graduate School of Library and Information Science. Mr. Updegrove serves as the University's Chief Information Officer and directs a staff of 375 providing communications infrastructure, data center, enterprise information, collaboration, academic, and user support services for the largest U.S. campus, with an enrollment of over 51,000 students. Prior to arriving at UT in January, 2001, Mr. Updegrove served as Chief Information Officer at Yale University; Associate Vice Provost for Information Systems and Computing at the University of Pennsylvania; Vice President of Educom (predecessor to Educause); Research Associate at Yale and the National Bureau of Economic Research; and Teaching Associate at Cornell University, where he studied industrial engineering and urban planning. Mr. Updegrove is active in Educause (chairing the Advisory Group on Administrative Information Systems and Services and co-chairing the Task Force on Computer and Network Security); Internet2 (serving on the Network Policy and Planning Advisory Committee); Texas GigaPOP (serving on the Board of Trustees); and the Southeastern Universities Research Association (serving on the IT Steering Group); and represents UT within the UT System as well as in the Coalition for Networked Information, Common Solutions Group, and Big 12 CIO group. He has lectured and consulted widely in the U.S. and abroad on IT strategic planning, networking, computer-based planning models, and computer gaming simulation. He currently serves on advisory committees for Apple Computer, Dell Computer Corporation, and Microsoft and on the board of directors of Knowbility, an Austin non-profit advocating barrier-free IT.

Moderator:

BOB RAY SANDERS is a professional communicator with major achievements in print journalism, public broadcasting, and higher education. Sanders is a columnist for the Fort Worth Star-Telegram. In two decades in public broadcasting, he served as vice president of KERA-TV, Channel 13 in Dallas-Fort Worth and as host and producer of the station's award-winning public affairs program, "News Addition." He is also a distinguished lecturer at Texas Woman's University. A past president of the Press Club of Fort Worth, he is also a member of the Society of Professional Journalists, the National Association of Black Journalists, the Press Club of Dallas, and the Dallas-Fort Worth Association of Black Communicators. Sanders has served as moderator for several Dallas Teleconferences, including "The REAL Cost of Online Courses," "Cheating and Plagiarism Using the Internet," "A.D.A. Issues and Requirements," "Improving Multimedia and Online Courses With Instructional Design," "Crisis on Campus: Will Your Emergency Plan Work?" "Surviving and Thriving in Your First Online Course," "Control, Conflict and Courseware: Intellectual Property in Online Education," "Are You History? Faculty Job Security in an Online World," "How to Customize an Online Course," "Online Testing: Assessment and Evaluation of Distance Learners," "Libraries, Copyright and the Internet," "Faculty Pay in Distance Education," "Teaching at a Distance: A Faculty Workshop with Tom Cyr," "The Learning Revolution in Higher Education," "Dancing on the Edge of Chaos," "Coping with Changing Campus Culture," and "Anger in the Classroom."



**"THE GROWING VULNERABILITY OF CAMPUS NETWORKS:
As attacks increase, colleges face tough, expensive
challenges in keeping intruders out"**

By Florence Olsen

The days when computer hacking was no more than an inconvenience to colleges --if an expensive one --could be over. A spokesperson for the U.S. Health and Human Services Department said last week that its auditors are checking the security of computer networks at several university research labs in response to heightened concerns about bioterrorists' possibly obtaining information about hazardous materials.

On top of national-security concerns, the volume and intensity of security incidents on campus networks are growing at a pace that raises questions about the adequacy of security precautions. Virus infections, unsecured software, and a shortage of people who know how to make computers safe on the Internet are converging to make campus networks a particularly alluring target for hackers, and now, some experts worry, terrorists.

Michael A. McRobbie, vice president for information technology at the Indiana University System, says colleges have a well-deserved reputation for lax network security. As a result, he says, they risk increased insurance costs and expensive lawsuits.

Attacks on networks to collect passwords, gain access to unauthorized data, install malicious code, or share bootleg movies are wasting crucial public resources and reducing productivity, Mr. McRobbie said in a stinging critique delivered last year to the annual meeting of Educause, the educational-technology consortium. In a time of increased national-security concerns, he said, pressure is mounting on colleges to gain better control of their computer networks, or risk losing federal grant money for research.

Taking Responsibility

"In the present climate of cyber-threats," Mr. McRobbie added in his speech, "somebody in the university has to step forward and take responsibility for trying to remediate these threats and to translate what the risks are."

Recognizing the problem, some colleges report that they are tightening security on their networks. Congress has proposed more money for research and education to help institutions improve the security of their networks. Software vendors, too, have reacted to the crisis: Microsoft, whose products are frequently targets of viruses, worms, and other destructive agents, in January announced a campaign aimed at making all of its software more secure.

According to Garland Elmore, technology dean of Indiana University-Purdue University at Indianapolis, a wave of viruses and computer-cracking attempts about four years ago was aimed at centrally located servers, the best-protected ones on campuses. Those threats were thwarted. Since then, he says, attempted computer and network-security violations have become more frequent and have affected more people --"now we're getting these kind of attacks all over the institution." And colleges have not yet seen the worst of it, he predicts.



One example is Nimda, an Internet worm, which hit colleges especially hard last fall --clogging networks and taking control of infected computers. At Indiana, where Mr. McRobbie is also chief information officer, security technicians found 600 computers on its networks that had the security hole that leaves computers open to attack from Nimda. The technicians were able to block most of the unsecured machines from other parts of the network until someone patched the holes.

Some smaller colleges were not as prepared to respond. After Nimda hit Central Wyoming College, which has 600 campus computers, officials closed down the college on a Friday to let its staff of eight technicians start cleaning up the mess. It took a week.

Viruses propagate more quickly these days, because there are more high-speed networks to carry them. About 50,000 viruses exist today, and that number could double by 2004, Mr. McRobbie says.

As viruses and worms have become increasingly complex and damaging, the computers that students bring to campus have been among the hardest hit. College technicians help faculty and staff members install antivirus software, but students often are on their own. Gordon D. Wishon, chief information officer and associate vice president at the University of Notre Dame, says students there are given free antivirus software and tips on its use. But many of them fail to configure the software to be updated as new viruses are created and propagated, he notes.

Security breaches are clearly on the rise.

The CERT Coordination Center at Carnegie Mellon University, which coordinates emergency responses to computer-security problems, recorded more than 52,000 incidents in 2001, each one involving as many as thousands of sites, including those on college campuses. By contrast, only about 22,000 incidents were reported in 2000.

'Script Kiddies'

One type of automated attack has become increasingly worrisome and time-consuming for colleges, says Robert E. Mahoney, a senior network engineer at the Massachusetts Institute of Technology. "Script kiddies," as the attackers are called, use scripts --easily executed programs --to break into unsecured computers. Such automated attacks can easily let a 15-year-old control more computers than he knows what to do with, Mr. Mahoney says. "We've seen certain scenarios on Internet relay chats where they are traded just like baseball cards --' I'll trade you 10 machines at MIT for some machines at the University of California."

Last March, MIT itself may have narrowly escaped becoming the launching point for a cyberattack on computers elsewhere. One night, someone on the Internet gained access to 33 computers in several research labs at MIT. Technicians noticed the invasion the next morning, after a security weakness had been discovered in the Solaris operating system. They found that a hacker had already exploited the flaw, leaving the computers open to be used in a "zombie" attack. Zombies --machines that have been infected with attack programs --are ordered by remote control to barrage other computers on the Internet with electronic messages. The technicians thwarted any potential damage when they pulled the computers offline and replaced the operating systems with clean versions.

Indiana's Mr. McRobbie says the method is favored by adolescent hackers, who amass "armies of hundreds, if not thousands, of zombies that they can wake up and use for denial-of-service attacks." Such attacks slow down or completely halt legitimate traffic that tries to enter or leave a Web site.



Two years ago, a 17-year-old hacker nicknamed Mafiaboy, from Montreal, received a criminal sentence for his role in attacks on Amazon.com and eBay. He had turned research-lab computers at several California universities into zombies and ordered them to attack the companies' Web sites. But his case was exceptional. While security managers might discover that a certain account on a particular machine was involved, rarely do they learn whose hands were on the keyboard.

Fear of Lawsuits

Colleges could be subject to costly negligence lawsuits if their computers are used in future attacks, or if sensitive information about students is stolen from campus computers, some experts say. Tracy Mitrano, policy adviser and director of computer law and policy at Cornell University, says courts may find colleges liable for an attack that used their machines, because campus officials should have known that unsecured networks were open to attack.

Campus networks are more vulnerable to attack than, say, corporate networks, because colleges need open networks for collaboration and access to information. It's rare for a college to have a strong firewall around its network. Such firewalls, because they block all but a few approved outsiders from gaining access, tend also to block collaborative researchers from other institutions. The vulnerabilities of campus networks "come from a good place, if you will," Ms. Mitrano says.

United Educators, a member-owned insurance company for colleges, says it does not yet offer a cyber-risk policy, even though that is one of the insurance industry's hot new areas for insuring clients. Instead, the company is advising its members to develop policies that will help reduce their networks' security risks. "Don't rely on insurance as a substitute for risk management, because risk management really is your front-line protection, even in the event of a lawsuit," says Frank Vinik, a United Educators risk manager.

College officials say they control only some of the conditions needed to promote better network security. Most software is sold with its security features turned off. Technical managers say they are overwhelmed by the number and complexity of advisories warning them of security flaws that require them to install software patches and updates. Administrators also say that students and faculty and staff members have all come to expect convenient access to information on campus servers, even when the users are miles away from the campus. Furthermore, the promise of improved network security in the form of digital certificates and a public-key infrastructure has been slow to materialize.

Daniel A. Updegrove, vice president for information technology at the University of Texas at Austin, says his biggest nightmare is knowing that only part-time or no systems administrators at all are available to control access to many student-owned and research-lab computers on the campus, or to keep up with security patches and updates. "So many computers within a university are managed casually," he adds, "that it's extremely hard to know who on the Internet has bona fide access to any of these computers."

Who Has Access?

He worries especially about research computers that have become obsolete. Such computers, purchased with grants, may have operating systems --Solaris 2.0 or SunOS 4.1.1, for example --that are no longer supported by the vendors that made them. Universities, researchers, and grant-making agencies "have systematically underinvested" in the protection of research computers, Mr. Updegrove says, and nobody wants to acknowledge that many general-purpose machines in campus labs are so outdated that they can no longer be secured. But then, he notes, most universities do not have budgets to pay for researchers' hardware and software, much less to pay full-time salaries for systems administrators in those labs. Typically, graduate students receive part-time salaries out of research grants to maintain lab computers.



Campus computing officials say they are hopeful that government money may help solve some of these problems. HR 3394, a computer-security bill that has passed the U.S. House of Representatives and has been referred to the Senate, authorizes \$878-million for undergraduate and graduate education and research on the best ways to protect computers and networks from viruses, criminal hackers, and, as emphasized by the bill's sponsor, terrorists.

"In the longer term, we need cost-effective ways to build systems that don't have security holes," says Carl E. Landwehr, director of the new trusted-computing program at the National Science Foundation, which supports research on more-secure computer systems. Considerable work in software engineering in the past 20 years has produced some knowledge about how to build systems with strong security, he says, but the computer industry hasn't succeeded in building those techniques into systems that most people buy. A high priority, he says, should be figuring out "how to build systems that don't require so much manual configuration and so much expertise on the part of systems administrators to keep them in a secure state."

If the Microsoft Corporation sticks to its new and, some say, belated security campaign, it would almost certainly mean that the company could not release new software as frequently as it does now; it takes more time to build secure software. Some Microsoft users in academe say that might not be such a bad thing. "It's the Microsoft environment that we're all scrambling to correct," says Cornell's Ms. Mitrano. In a recent memo to employees about security flaws in Microsoft products, the company's chairman, Bill Gates, acknowledged that it "can and should do better."

Progress at Virginia Tech

Virginia Tech is ahead of the curve in making its computers and networks more secure. Other institutions are now using some of the tools and procedures that its security experts helped to develop. Technology managers there say they have spent the past seven or eight years trying to come to grips with network vulnerabilities --and the time spent on security-awareness seminars and using security tools seems to be paying off. In the past six months, only two or three attacks against the network have been successful, says Randy Marchany, who runs Virginia Tech's new security lab. While the number of attempted attacks on the network has increased sharply in the past couple of years, he says, the number of successful attacks has stayed constant.

The university's security technicians use the same scanning tools that hackers use to find security holes on networks. If the tools detect a computer that has been "compromised," technicians immediately take that machine off the network. Most colleges do not use such tools, because they require someone skilled to interpret the results. Besides, for many institutions, a decision to scan people's computers --even if only to find vulnerabilities --goes against the grain. At Virginia Tech, all computer platforms --including those for scientific instruments --and their software configurations are also tested and rated as to whether they are secure enough to be put onto the network.

This past year, Virginia Tech also stepped up efforts to improve the skills of systems administrators. Last fall, more than 300 such staff members, from Virginia Tech as well as other colleges in Virginia and neighboring states, attended a free, three-day seminar on computer security and forensics given by Virginia Tech and the SANS Institute, an organization for network administrators and security officers.

Informal user groups and casual seminars set up to raise security awareness are also useful. At least, Mr. Marchany says, he sees better results from those activities than from what he calls "central directives."



"If you put out a memo and say, 'This is what you should do,' that doesn't work. But if I say, 'Hey, I'm offering a class,' and in the class I tell them what I would have told them in the memo, it works."

Such training seems likely to grow in importance. Last August, Virginia Tech spent \$100,000 on four servers equipped with filters to remove viruses from e-mail coming into and leaving the university network. It was money well spent, Mr. Marchany says: "Sometime in November, we intercepted our millionth virus."

NETWORK INCIDENTS AT ONE UNIVERSITY

Many colleges are reporting increases in hacking, illegal acts, or other destructive incidents involving their computer networks. One research university, which asked not to be identified, provided the following data, showing the changes in the kinds of incidents commonly experienced in 1999 and 2001. Figures reflect incidents reported in the month of December for the two years.

Commercial use of the campus network - Definition: Use of university Web pages to sell products or services
1999 : 1 2001: 0

Copyright infringement - Definition: Unlicensed or unauthorized copying of copyrighted materials
1999 : 2 2001: 1

Denial of service - Definition: "Flood" of messages released with the intention of slowing or stopping other network traffic
1999 : 1 2001: 1

Violation of Federal Educational Rights and Privacy Act - Definition: Failure to protect the privacy of students' personal information
1999 : 0 2001: 1

Fraud - Definition: Financial scheme to defraud victims, such as a chain letter
1999 : 5 2001: 2

Hacking/machine hacked - Definition: Writing a program to gain unauthorized access to a computer
1999 : 6 2001: 6

Harassment - Definition: Conduct that is unwelcome or intimidating to the victim
1999 : 0 2001: 1

Inappropriate bandwidth use - Definition: Excessive nonacademic use of the network for downloading or transferring large files
1999 : 0 2001: 13

Malicious code attacks - Definition: Harmful software programs, such as viruses, that destroy files, steal passwords, or otherwise cause damage
1999 : 0 2001: 42

Open mail relay - Definition: Use of university computer to relay mail from one address outside of the university to another outside address
1999 : 3 2001: 3



Port scanning - Definition: Hostile Internet searches for open "doors," or ports, through which intruders gain access to computers
1999 : 5 2001: 12

Spam - Definition: Mass mailing of unsolicited or unwanted e-mail
1999 : 17 2001: 30

Total, December 1999: 40

Total, December 2001: 112

Copyright 2002, The Chronicle of Higher Education. Reprinted with permission.



**“SCALE THE SOLUTION TO THE PROBLEM
Campuses need to move proactively to
meet growing information security demands”**

By Cedric Bennett

The only way of discovering the limits of the possible is to venture a little way past them into the impossible.¹—Arthur C. Clarke

The Internet is a remarkable tool and change agent that has been successfully leveraged by colleges and universities to support, enhance, and extend the teaching/learning process; the creation of new knowledge through research; and the increasingly complex business of managing and administrating our institutions. Moreover, it has become an indispensable communications mechanism through which we reach students, faculty, staff, donors, alumni, applicants, granting agencies, vendors, the public, and others.

At the same time that the Internet has become a mission-critical resource, it has also introduced new and growing responsibilities. Although it supports and even creates new ways to enhance the education process, this virtually unregulated communications medium has also become a costly management burden. It is becoming a more difficult environment to use safely—the ability to reach out to the rest of the world also invites the rest of the world to reach back, sometimes in very unsettling ways. And, as if the threat of unprovoked cyber attack were not enough to manage, federal and state legislation designed primarily to protect individual privacy has been demanding additional resource allocation with increasing frequency.

Increasing Cyber Threats

Ever since Robert Morris wrote the first computer worm in 1988,² information-security experts have been both observing and defending against a growing number of Internet attacks. What is becoming increasingly clear is that the level, sophistication, speed, and time-to-exploit of autonomous Internet-based attacks are escalating. A few examples of the increase of serious and debilitating network exploits occurring in 2003 alone illustrate how grave the situation has become:

- **Speed of delivery**—The MS SQL Slammer worm traversed the entire Internet and did nearly all of its damage in less than 15 minutes, whereas previous rapidly spreading exploits took multiple hours or days to infect targets worldwide.
- **Vulnerability of private information**—The BugBear virus/worm showed just how vulnerable our institutions' widely distributed data is by sending very private or confidential letters and files, located on campus-wide desktop computers, to unauthorized recipients all over the world.
- **Sophistication and speed of delivery**—SoBig showed just how easily and rapidly an e-mail-delivered virus/worm could evade antivirus software and invade and replicate itself onto nearby machines.
- **Sophistication of payload and time-to-exploit**—Blaster, and nearly a dozen other MS RPC exploits, began appearing only two weeks after the vulnerability had been announced and the patch made available by Microsoft,³ and it delivered a very sophisticated, multi-pronged, and expensive attack.⁴



Increasing Unfunded Regulatory Mandates

Most universities and colleges are aware of the FERPA regulations regarding the protection of certain elements of student information; these requirements have been a well-known part of the higher education regulatory environment for multiple decades. However, within the past several years federal legislation (and in some cases state legislation) has added an almost debilitating array of additional privacy and security requirements. Some of the major ones follow:

- FERPA—Family Educational Rights and Privacy Act of 1974; also known as the Buckley Amendment
- HIPAA—Health Insurance Portability and Accountability Act of 1996
- DMCA—Digital Millennium Copyright Act of 1998
- GLBA—Gramm-Leach-Bliley Act of 1999
- USA PATRIOT Act—Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
- TEACH Act—Technology, Education, and Copyright Harmonization Act of 2002

Others, less recent but still very significant, include the Electronic Communications Privacy Act of 1986 and the Computer Fraud and Abuse Act of 1986.

Each of these federal laws includes both management and information technology requirements. In some cases, there are even new institutional roles required (such as privacy officer, security officer, security plan coordinator, and notification of claimed infringement agent). Congress does not seem to feel that they have finished this work; more legislation requiring even more attention to privacy and information security is being proposed and considered today.⁵

Shifting Toward a Proactive Stance

As these threats and compliance requirements have increased, more and more of our institutions have focused on improving their information-security posture. Probably the single greatest movement forward has come about as a result of shifting to a proactive stance. Instead of just reacting to problems and incidents as they occur, colleges and universities are starting to think in terms of anticipating issues and working to prevent them. Another major shift forward has come from a growing realization that information security and regulatory compliance is not just a technology issue but is broadly institutional and very people-focused.⁶

Some of our institutions have designated specific individuals as security officers and created small teams to focus on information security. Others have assigned the information-security role as a collateral duty of one or more staff members. No matter how the function is staffed, those individuals charged with attending to information security and compliance are adopting a variety of approaches to leverage their resources and technical expertise, all aimed at improving the information-security posture of their institution. They know they don't have sufficient resources to meet all challenges alone; many of the solutions these information-security leaders choose include creating and leveraging strategic alliances with others across their institutions. What follows are examples of some key approaches being applied.

Build Alliances

Wise information-security officers understand that other staff offices within the institution are also responsible for aspects of compliance, protection of data, development of policy, interpretation of law, and like activities. Some of these functions may be staffed within the college or university, and some



may be outsourced. In addition, there are often committees made up of faculty, students, and staff with advisory or oversight responsibilities in at least some of these same areas. The organizational names may vary, but they usually cover such functions as internal audit, general counsel, compliance, risk management, and public safety.

In any case, no matter what they are called or how they are staffed, these are key offices engaged in information-security@related activities. At the very least, they are experts in specific disciplines, which can be useful in providing crucial answers or interpretations to questions of law, business, risk, research, security, and so on. From a more strategic perspective, they can also become partners in helping to present and support information-security solutions to other campus leaders.

Identify Key Data Owners

Major administrative offices in most institutions are responsible for much of the institution's data, which can include (but is not limited to) financial, personnel, student, fund-raising, investment, and compliance data. Just as critical, but often far less centrally managed, is research data, course data, and other intellectual capital of the institution or individuals.

The individuals and offices charged with the responsibility for institutional data care a great deal about its protection. Because they are not focused primarily on information security, however, they often are not aware of the variety of cyber threats that may exist. Security officers who have invested the time to identify, meet, and educate these leaders usually find them willing allies in presenting and implementing information-security measures.

Create Partnerships

Others outside of the central security organization have both responsibility for and expertise with information security—at least with regard to their specific responsibilities. These individuals may work in other parts of the central computing organization, or they might be located in widely distributed parts of the institution in academic or administrative organizations or research laboratories. Establishing liaison with these individuals goes a long way toward extending the knowledge and influence of any central security organization. Developing these distributed experts into a peer group that shares information, deals with serious emergencies, and reviews ideas for improving information security works to overcome the boundaries that can otherwise prevent meaningful dialogue and cooperation.

Similarly, connections can be established with other information-security practitioners working in other institutions, so that difficult questions can be considered from a variety of perspectives. Joining online discussion lists like the EDUCAUSE Security Discussion Group (<http://www.educause.edu/security>) or attending annual conferences like the EDUCAUSE/Internet2 Security Professionals Workshop (<http://www.educause.edu/conference/security/>) are excellent ways to meet and leverage the expertise of others working on similar problems at other institutions.

Set Institutional Policies

Every information-security officer knows that policies alone don't stop hackers or protect institutional data. But effective information-security officers also know that policies create the context and the foundation for developing the practices that can accomplish those goals.

Establishing institutional policies can be a time-consuming job. The advantage, however, is that not only do these important policies get written and accepted, the very process can help in raising awareness and educating others.



Raise Information Security Consciousness on Campus

Raising awareness of information-security issues across the campus is a must. The goal is not to make every computer user an expert in information security. Rather, the effort aims to make every computer user aware that information security is an important issue and one in which each of them must play a role. The objective is to help develop simple but effective habits that will raise institutional information security—similar to an educational campaign to make sure everyone uses a deadbolt to lock exterior doors on their homes.

Increase Technical Expertise

Security officers know that they cannot raise the level of campus information security single-handedly. Just as it is important to raise overall awareness of information security across the institution so that each individual can contribute to the solution, it is critical to raise the level of detailed information-security expertise among technical staff. Only through such education and training will more effective practices be broadly exercised in the deployment of both central and distributed information resources. The information-security staff will normally be the experts to those experts—it is the system administrators, programmers, database administrators, and others who will successfully follow effective practices that ensure a successful information-security program.

Only Deploy Technologies with the Greatest Leverage

Technology is important to successful information security, but it does not play as major a role as the issues mentioned above. Vendors often promise wonderful results from the simple deployment of their hardware or software solutions. Security officers understand that they should only deploy technology with proven value that can be managed with a minimum of resources.

Reexamine Underlying Assumptions

In most of our institutions, approaches to information security have not kept pace with the problems. As the examples provided at the beginning of this article illustrate, the growth in the scale, scope, tenacity, and costs of the issues we face are all rapidly increasing. It is unlikely that minimalist, reaction-based, or single-point-oriented solutions will succeed in addressing these complex problems. Moreover, such solutions will almost certainly not prove effective against problems we have yet to see.

The more broadly based approaches outlined in the section above have greatly helped the institutions implementing them. They are both proactive and strategic in approach, which tends to help in the development of solutions that are more general and effective over a larger set of problems. Still, these information-security solutions are frequently implemented in a general atmosphere that is not particularly tolerant of what are often perceived to be unnecessary and bureaucratic restrictions.

In higher education there is often a natural tension between the fundamental mission and culture of the institution, which encourages and thrives on open sharing and communication, versus the fiduciary and legal requirements of those same institutions to keep certain kinds of information resources secure and confidential. This tension has been balanced and handled with varying degrees of success at different institutions. On some of our campuses there is an understanding that it is important at least to acknowledge the tension and recognize that there will be times when both of those requirements may not be fully served.

It is important to begin discussion on our campuses aimed at developing a strategy that meets the institutional need for information security and also supports the requirements of the institution to suc-



cessfully pursue its fundamental mission of teaching, learning, research, and public service. Such a discussion will not be easy to start or maintain; it is a leadership task that will take collaborative effort across the entire institution. It will include addressing knotty issues:

- Reconsidering decisions made in the past, when threats and requirements were not as severe as they have become today
- Confronting conventional wisdom about the specific requirements for openness and the real versus imagined constraints imposed by information-security technologies
- Developing institutional information-security policies and an information-security architecture
- Recognizing that sensitive information exists in digital form all across and even beyond the campus, from highly secure servers to traveling laptop computers
- Discovering where real needs exist for reduced security (for example, specific research projects) and providing such facilities while protecting all other resources
- Acting from the understanding that information security is more a people issue than a technical one and that education and communication are a major part of any solution
- Seeking ways to support information-security requirements that are engineered to minimize both dependence upon individual conformity and overly oppressive controls

Each institution will need to find the solutions that best suit its own values and goals as well as its legal requirements, view of acceptable risk, and budget constraints. These discussions can be guided by a set of principles recently articulated by a National Science Foundation-sponsored workshop organized by the EDUCAUSE/Internet2 Computer and Network Security Task Force:⁷

- Civility and community
- Academic and intellectual freedom
- Privacy and confidentiality
- Equity, diversity, and access
- Fairness and process
- Ethics, integrity, and responsibility

A major advantage of this effort to develop an institutional information security strategy is the knowledge that the outcome will be an informed institutional decision that is owned and understood throughout the campus.

Probably the best news is that general attitudes about the need for information security are shifting more toward the positive. The members of our community and our institutional leaders are becoming more acutely aware of just a few of the serious consequences of inadequate protection or insufficient regulatory compliance. Many are now ready to support recommendations that will lead to a more secure information environment on our campuses.

Our campuses now need information-security leaders with the courage to start the difficult dialogue, the understanding to keep the conversation focused on institutional requirements, and the insight to manage the discussion within that institutional context.

Endnotes

1. Clarke's "second law," from A. C. Clarke, *Profiles of the Future: An Inquiry into the Limits of the Possible* (London: Gollancz, 1999, updated edition).
2. On November 2, 1988, Robert Morris, Jr., a graduate student in computer science at Cornell University, wrote an experimental, self-replicating, self-propagating program called a worm and injected it into the Internet.



3. By comparison, the MS SQL Slammer worm of early 2003 exploited a vulnerability for which a patch had been available for six months.
4. Many relatively well-prepared universities saw upwards of 30 percent of their Windows machines infected by the MS RPC exploits. The cost of repair plus the cost of lost productivity for these institutions is in the multi-million-dollar range.
5. I do not argue that such legislation is inappropriate or unnecessary, only that it is increasing the information-security management and cost burden of our institutions.
6. D. Ward, "Letter to Presidents Regarding Cybersecurity," ACEnet, Eye on Washington, Feb. 28, 2003; on the Web at <<http://www.acenet.edu/washington/letters/2003/03march/cyber.cfm>>.
7. EDUCAUSE/Internet2 Computer and Network Security Task Force, "Principles to Guide Efforts to Improve Computer and Network Security for Higher Education," August 2002; on the Web at <<http://www.educause.edu/ir/library/pdf/SEC0310.pdf>>.

Cedric Bennett (Ced.Bennett@stanford.edu) is Emeritus Director, Information Security Services, at Stanford University in Stanford, California, and still spends considerable time helping Stanford and other institutions address their information security requirements.

Educause Quarterly Volume 27, Number 1, 2004
Used by permission.



A(n Extended) Campus Information Security Conversation by Daniel Updegrave

Wherein the Chairman of the Department of Molecular Gerontology (MG) at a large university <bigu.edu> phones the university's **Information Security Officer (ISO)**.

MG: Hello, is this the Information Security Office? Our departmental server here in Molecular Gerontology is running very slowly, and students and faculty are complaining to me daily that they can't get their work done. As you may know, Joe Smith, the wizard grad student who architected our network and ran the server so expertly left last year, and the new student we've assigned, Bill Jones, can't seem to diagnose the problem.

ISO: Sorry to hear about your problem. We'll send, Susan Gonzales, one of our information security analysts over to have a look right away. Can you have Bill meet her to review the problems?

MG: Well, actually, Bill is in Europe on a research project, but Mary, our departmental business manager can unlock the door of the computer room.

**** A few hours later ****

ISO: This is the Information Security Officer. May I speak with the Chair, please.

MG: Speaking. Thanks for getting back to me. Since we talked I've had three more complaints. Have you been able to resolve the problem?

ISO: Well, Susan's work was hampered by not having access to the system logs and the administrator password that Bill could have provided, but she was able to make a preliminary diagnosis.

MG: Great! How soon before we're back to business as usual?

ISO: Well, that's hard to say. Based on observation of Mary's logging in, Susan noted that the version of the Operating System is two years old and so has not had several recent security patches installed. Susan also reported that servers running this version of the OS have been the target of attacks around the Internet recently, including several on campus. These attacks follow a common pattern, exploiting a well-known vulnerability in the "sendmail" program to gain root access.

MG: What exactly does "root access" mean?

ISO: You can think of root access as having complete control of the system, including all programs installed, all user accounts, and all user data.

MG: But what does this root access have to do with poor performance of the server?

ISO: Well, it could be several things. One or more rogue processes running, perhaps a password sniffer, an open FTP, or an IRC bot. Also it appears there's nearly no disk space left on the system, which could indicate that one of these rogue programs is malfunctioning, or perhaps uses substantial disk storage as part of its operation.

MG: How soon can Susan clean this up and get us back to work?



ISO: Too soon to tell. Partially it depends on whether we can reach Bill to get the root password.

MG: Can't you just call the computer vendor and ask them for emergency help?

ISO: Well, that's a bit awkward, since the version of the OS you're running is no longer supported by the vendor. Moreover, Mary advised us that your systems are not under a maintenance contract. I will ask Susan if she can stay late this evening to explore this further.

MG: Thanks. Please keep me informed. Here's my home number. I'll have Mary try to track down Bill.

**** Later that evening ****

ISO: Good news and bad news: Good news is that we didn't need Bill to obtain root access. The root password was set to "gerontology," which Susan guessed after several tries. The bad news is that you do, indeed have a root penetration on your hands, and the cracker installed a sniffer on your Ethernet interface. The reason you're out of disk space is that the sniffer's log file has gotten so big, since it's been running for about ten weeks.

MG: Well, I'm glad the password was easy to guess!

ISO: Frankly, if it was easy for Susan to guess, it may have been the way that root access was obtained by the cracker.

MG: I see what you mean. Now what exactly is a sniffer?

ISO: It's a program that monitors traffic on the Ethernet interface, looking for character strings that appear to correspond to login IDs and passwords. These combinations are logged, and from time to time, the cracker harvests the data for future use. Apparently he or she got careless and forgot to delete the log file.

MG: Well, now that Susan has done her job so expertly, let's have her delete the log file, change the root password, and get everyone back to work. What a relief!

ISO: Unfortunately, it's not that easy. We can't be sure that the cracker didn't install a backdoor program to obtain root access, so we'll have to take the server off the network, reinstall the operating system and all the security patches to the OS, reinstall the application programs and their security patches. Then, since all the user passwords are compromised, we'll have to have all users change their passwords, not only for this server, but all other systems they log into, here and at other universities.

MG: How long will this take?

ISO: Best guess would be three days for the server work. The password changes could be done in parallel.

MG: That's out of the question! We have students preparing for mid-terms and a major proposal due to NSF next week. We'll just have to put up with the slowness until these deadlines are past. Then we'll get people to change their passwords and get Bill to fix the server.

ISO: Sorry, we can't allow a compromised system to remain on the network. We'll have to disconnect you from the campus network this evening.



MG: You can't be serious! You say it's been compromised for ten weeks. What's the risk of its remaining on the network for another week or two, until the academic crunch is passed? There are no sensitive University data on that server anyway, only email and some doctoral research.

ISO: The risks are actually quite high: Data on the server could be deleted or altered, email could be sent in the name of any of your users, and the system could be used as a launching point for attacks on computers here or elsewhere.

MG: Launching point for attacks? That sounds pretty far-fetched.

ISO: Actually, computers at Stanford and UCSB were used last year to launch so-called "denial of service" attacks on several key commercial sites, such as eBay and Amazon.com.

MG: We can't function for a day without email!

ISO: Well, that's comparatively easy: Our central email server is pre-programmed to provide email for all faculty, staff, and students. For some reason, however, your department has elected to run its own email server. We can activate accounts for all your folks by 9:30 tomorrow morning.

MG: Thanks, but will they all have the proper address, of <firstname@mol-gero.bigu.edu>?

ISO: Sorry, you'll have to settle for <first-last@bigu.edu>, which is our standard format.

MG: But we've always been "mol-gero.bigu.edu." It's this sort of inflexibility that led us to run our own server in the first place.

ISO: Well, perhaps we can address this issue after we get your server back on the air. Now what account should Susan's overtime be charged to?

MG: This is outrageous! You take us off the network and then charge us to help us get back on?

ISO: Well, perhaps we wouldn't be faced with such extreme measures if your department hadn't elected to run its own server without professional administration, ignored three messages from this office alerting you to the server security vulnerability, and failed to attend our quarterly information security update meetings. We much prefer to engage proactively rather than in crisis mode. Now what was that account number again?

MG: Mary will provide the account number in the morning, and I'll be calling the Provost as well. With all the indirect cost recovery this department generates, I can't believe the central administration let's us be exposed to such risks!

This skit was developed for the Computer Policy and Law Annual Seminar, Cornell University, July 2001. It has been featured in numerous conferences and seminars, including Educause, October 2001 (Indianapolis); Coalition for Networked Information, December 2001 (San Antonio); University of Texas System Information Security Officers (Austin); National Association of College and University Attorneys 2002 (Boston); CUDI, October 2002 (Ciudad Juarez, Mexico); Educause Security Task Force, October 2002 (Washington); and elsewhere. A published version is available at *Educause Quarterly*, Vol. 25 No. 2, 2002 <<http://www.educause.edu/ir/library/pdf/eqm0221.pdf>>. URL = <http://wnt.utexas.edu/~danu/security-skit.html>



Activities:

1. Take the free National Cyber Security Alliance Stay Safe Online - Security Fundamentals Course available at: <http://www.staysafeonline.info/enroll.adp>.

Course Description

“This free course will provide you with an introduction to and a general awareness of computer security related issues. It will allow you to identify what you can do in your role within your organization or at home to protect your networks, systems, and information against cyber attacks.”

Learning Objectives

“By the end of this course, you will be able to:

- Identify your role in protecting information systems
- Identify security threats, vulnerabilities, countermeasures and risks
- Report risks appropriately
- Identify, report, and react to viruses
- Practice good password management”

2. Conduct the Risk Analysis available at the security web site at Virginia Tech: Play It Safe: Risk Analysis (STAR). <http://security.vt.edu/playitsafe/index.phtml#RiskAnalysis>.

Risk Analysis (STAR)

Why do a risk analysis for your information technology assets? Who will it benefit? The Security Targeting and Analysis of Risks (STAR) process is one that will benefit both the individual department and the university as a whole. Completing such an analysis is extremely important in today's advanced technological world. It is important that users understand what risks exist in their information technology assets environment, and how those risks can be reduced or even eliminated.

3. Evaluate your cybersecurity in terms of the SANS Institutes Top 20 List: Most Critical Internet Security Vulnerabilities - The Experts Consensus. <http://www.sans.org/top20.htm>.
 - Which vulnerabilities, if any, is your institutions system laden with?
 - If there are vulnerabilities present, identify the appropriate steps to alleviate these problems. The SANS list provides both flaw and fix.

Discussion:

4. Experts agree that cybersecurity is a matter not just for the technology staff, but for all computer users on campus.
 - What are some of the ways that computer users who are not particularly technology-savvy can put the institution at risk for cybersecurity breaches?
 - What are some of the things that computer users who are not particularly technology-savvy can do to improve cybersecurity on campus?
 - How do you get security policies and procedures information into the hands of the general user, and how can you encourage them to follow these policies?



Dallas Teleconferences Web Site
<http://telelearning.dcccd.edu/prodsvcs/Teleconferences/default.htm>

“CyberInSecurity? Prevention and Protection Solutions” Teleconference Web Site
<http://telelearning.dcccd.edu/teleconferences/2K32K4/cyberinsecurity/default.htm>

PBS Web Site
<http://www.pbs.org/als/live/>

Electronic Resources

NOTE: Links to the bolded items below are included on the Teleconference Web Site

Advanced Laboratory Workstation System/National Institutes of Health. Selecting Good Passwords.
<http://www.alw.nih.gov/Security/Docs/passwd.html>.

Arone, Michael. Hacker Steals Personal Data on Foreign Students at U. of Kansas. *The Chronicle of Higher Education*. January 24, 2003. <http://chronicle.com/free/2003/01/2003012403n.htm>.

Bennett, Cedric. Scale the Solution to the Problem: Campuses need to move proactively to meet growing information security demands. *Educause Quarterly*. Volume 27, No. 1, 2004.
<http://www.educause.edu/pub/eq/eqm04/eqm0410.asp>.

Bruhn, Mark and Petersen, Rodney. Planning for Improved Security. *Educause Review*. November/December 2003. http://www.educause.edu/pub/er/erm03/erm036_articles.asp?id=10.

Carlson, Scott. Report by MIT Researchers Says Unwanted Hard Drives Often Reveal Secrets. *The Chronicle of Higher Education*. January 17, 2003.
<http://chronicle.com/free/2003/01/2003011701t.htm>.

Carnevale, Dan. Security Lapses on Campuses Permit Theft From JSTOR Database. *The Chronicle of Higher Education*. December 12, 2002. <http://chronicle.com/free/2002/12/2002121201t.htm>.

---. Presidential Panels Report Calls on Colleges to Aid in Securing Networks. *The Chronicle of Higher Education*. September 19, 2002. <http://chronicle.com/free/2002/09/2002091901t.htm>.

The Center for Internet Security. <http://www.cisecurity.org/>.

Benchmarks.

Benchmark FAQ.

CERT Coordination Center. www.cert.org.
 Octave.

The Growing Vulnerability of Campus Networks. Colloquy Live with Randy Marchany. *The Chronicle of Higher Education*. March 13, 2003. <http://chronicle.com/colloquylive/2002/03/networks/>.

Educause. EDUCAUSE/Internet2 Computer and Network Security Task Force.
www.educause.edu/security/.



- . **Effective Security Practices Guide.** <http://www.educause.edu/security/guide/>.
- . National Strategy To Secure Cyberspace. <http://www.educause.edu/security/national-strategy/>.
- . Security Risk Assessment and Analysis Resources.
http://www.educause.edu/asp/km/term_resources.asp?Term_ID=665.
- Foster, Andrea and Jackson, Gregory A. Colloquy Live: The High Cost of Computer Worms. 18 March 2004.
<http://chronicle.com/colloquylive/2004/03/worm/>.
- InfraGard. <http://www.infragard.net/about.htm>.
- Luker, Mark. Statement on Behalf of Higher Education on Release of the National Strategy to Secure Cyberspace. <http://www.educause.edu/ir/library/pdf/NET0203.pdf>.
- National Cyber Security Alliance. Stay Safe Online - Security Fundamentals.**
<http://www.staysafeonline.info/enroll.adp>.
- National Institute of Standards and Technology (NAST). Guidelines on Electronic Mail Security.
<http://www.linuxsecurity.com/docs/PDF/PP-ElectronicMailSecurity-RFC.pdf>.
- . Procedures for Handling Security Patches. <http://www.linuxsecurity.com/docs/PDF/draft800-40.pdf>.
- Panetteiri, Joseph C. How Secure Are You? University Business. March 2004.**
<http://www.universitybusiness.com/page.cfm?p=472>.
- The Presidents Critical Infrastructure Protection Board. The National Strategy to Secure Cyberspace - Sept. 2002 Draft. <http://www.whitehouse.gov/pcipb/>.
- Salomon, Kenneth D., Cassat, Peter C., and Thibeau, Briana E. IT Security for Higher Education: A Legal Perspective.** <http://www.educause.edu/ir/library/pdf/CSD2746.pdf>.
- SANS Institute. What is the SANS Institute? <http://www.sans.org/aboutsans.php>.
- . **SANS/FBI Top 20 List: most Critical Internet Security Vulnerabilities - The Experts Consensus.**
<http://www.sans.org/top20.htm>.
- U.S. Cyber Security Weakening. <http://www.wired.com/news/infostructure/0,1377,49570,00.html>.
- Virginia Tech. Acceptable Use Guidelines. <http://www.policies.vt.edu/acceptableuse.html>.
- . Go To Class: VT Presentations/Papers.
<http://www.security.vt.edu/gotoclass/index.phtml#PresentationsPapers>.
- . Play It Safe: Protective Software (Plus More).
<http://security.vt.edu/playitsafe/index.phtml#ProtectiveSoftware>.
- . **Play It Safe: Risk Analysis (STAR).** <http://security.vt.edu/playitsafe/index.phtml#RiskAnalysis>.
- . Play It Safe: Selecting Good Passwords.
<http://security.vt.edu/playitsafe/index.phtml#SelectingGoodPasswords>.



Print Resources

- Carnevale, Dan. Network Practices Can Endanger Students Privacy, Report Warns. *The Chronicle of Higher Education*. November 23, 2001. <http://chronicle.com>.
- Eisler, David L. Campus Portal Security: Access, Risks, and Rewards. *Syllabus*. Vol. 16, No. 10. May 2003.
- Farrell, Elizabeth F. Hofstra U. Fires Employee Accused of Changing Students Grades. *The Chronicle of Higher Education*. February 26, 2002. <http://chronicle.com>.
- Foster, Andrea L. California Colleges Prepare to Disclose Computer Intrusions. *The Chronicle of Higher Education*. June 6, 2003. <http://chronicle.com>.
- . Colleges Brace for the Next Worm. *The Chronicle of Higher Education*. March 19, 2004. <http://chronicle.com>.
- . Computer-Crime Incidents at 2 California Colleges Tied to Investigation Into Russian Mafia. *The Chronicle of Higher Education*. June 24, 2002. <http://chronicle.com>.
- . Federal Officials Issue Alert on Security of College Networks. *The Chronicle of Higher Education*. July 5, 2002. <http://chronicle.com>.
- . ID Theft Turns Students Into Privacy Activists: Colleges respond by reducing reliance on Social Security numbers in databases. *The Chronicle of Higher Education*. August 2, 2002. <http://chronicle.com>.
- . Russian Mafia May have Infiltrated Computers at Arizona State and other Colleges. *The Chronicle of Higher Education*. June 20, 2002. <http://chronicle.com>.
- Lowery, Courtney. Florida Memorial College Fires 2 Workers and Expels 3 Students Amid Grade-Changing Inquiry. *The Chronicle of Higher Education*. July 26, 2002. <http://chronicle.com>.
- Luker, Mark and Petersen, Rodney, eds. *Computer and Network Security in Higher Education*. Educause Leadership Strategies, Volume 8. Jossey-Bass: San Francisco, 2003.
- Microsoft Admits Passport Security Flaw. *The New York Times*. May 8, 2003. www.nytimes.com.
- Olsen, Florence. The Growing Vulnerability of Campus Networks. *The Chronicle of Higher Education*. March 15, 2003. <http://chronicle.com>.
- . Network Administrators on Campuses Scramble to Fix Critical Security Flaw in Windows. *The Chronicle of Higher Education*. August 8, 2003. <http://chronicle.com>.
- . Security: Threats Will Get Worse. *The Chronicle of Higher Education*. January 30, 2004. <http://chronicle.com>.
- Read, Brock. Delaware Student Allegedly Changed Her Grades Online. *The Chronicle of Higher Education*. August 2, 2002. <http://chronicle.com>.



- . Hackers Steal Data from U. of Texas Database. *The Chronicle of Higher Education*. March 21, 2003. <http://chronicle.com>.
- Rooney, Megan. Point Park College Investigates Unauthorized Changes in Student Grades. *The Chronicle of Higher Education*. November 5, 2002. <http://chronicle.com>.
- Selingo, Jeffrey. Graduate Student is Charged With Hacking into U. of Michigan Computer System. *The Chronicle of Higher Education*. August 4, 2003. <http://chronicle.com>.
- Shoichet, Catherine E. Princeton U. Will Reassign Admissions Official Who Broke Into Yale U. Web Site. *The Chronicle of Higher Education*. August 14, 2002. <http://chronicle.com>.
- Schwartz, John. Decoding Computer Intruders. *The New York Times*. April 24, 2003. www.nytimes.com.
- Wade, Kent. IT Security on Campus: A Fragile Equilibrium. *Syllabus*. Vol. 16, No. 10. May 2003.
- Young, Jeffrey R. Princeton Admissions Official Breaks Into Yale Admissions Site. *The Chronicle of Higher Education*. July 26, 2002. <http://chronicle.com>.



UPCOMING PROGRAMS

(All times are 2:30 - 4:00 PM ET unless indicated otherwise)

APRIL 20, 2004	MAKING MENTORING ACCESSIBLE: INNOVATION AND TECHNOLOGY IN TEACHER INDUCTION
APRIL 21, 2004	THE TEXAS SUCCESS INITIATIVE
JULY 28, 2004	DISTANCE LEARNING NURSING RE-ENTRY PROJECT

Programs to be streamed and available via the Internet include:

APRIL 2004	CRITICAL THINKING: REQUIRED LEARNING FOR THE 21ST CENTURY
MAY 2004	CHEATING AND PLAGIARISM USING THE INTERNET
JUNE 2004	ETHICAL DECISION MAKING IN THE PROFESSIONAL SETTING --a special three hour in-service program for professional counselors and healthcare providers
JULY 2004	DOES YOUR ONLINE COURSE NEED EXTRA CREDIT TO PASS?
AUG. 2004	RETIREMENT PLANNING FOR EDUCATIONAL EMPLOYEES

VIDEOCONFERENCE TAPE ORDER FORM



STARLINK[®]

Videoconference Title: "Cyber Insecurity"

Videoconference Date: April 8, 2004

Registrant Name:

Title:

Institution:

Mailing Address:

Street Address:

Circle Method of Payment: *(Include PO number and attach copy of PO)*

Check

PO _____

Note: Purchasing organization does not have the rights to:

- 1) edit or alter this tape, except for classroom use.
- 2) use the materials in a broadcast, without obtaining written consent from **STARLINK**. College cable channel broadcasts are acceptable.
- 3) duplicate, sell or rent the materials.

Tape Format: 1/2 inch VHS

Videoconference Tape Fee:

\$18 STARLINK Members

\$36 Non-Members w/ License

**A tape of the videoconference will be shipped within 30 days
after receipt of the completed order.**

Please return this completed agreement to:

**STARLINK
LeCroy Center for Educational Telecommunications
9596 Walnut Street
Dallas, TX 75243-2112
Phone: (972) 669-6505 FAX (972) 669-6699**

VIDEOCONFERENCE EVALUATION FORM



EVALUATE "CYBERINSECURITY"

On a scale of 1-5, with 5 being the highest, rate the videoconference in terms of its value to you.

	Excellent			Poor	
Timeliness of topic	5	4	3	2	1
Program's format	5	4	3	2	1
Moderator	5	4	3	2	1
Panelists or Instructor	5	4	3	2	1
Handouts	5	4	3	2	1
Technical quality	5	4	3	2	1
Overall evaluation of program	5	4	3	2	1
Local site activities were held?	_____ YES		_____ NO		

1. Institution name: _____

2. My current position is: (circle one)

a. Faculty

c. Classified Staff

b. Administrator/Professional Staff

d. Other _____

3. What did you like most about the videoconference?

4. What could have been done to make it more valuable to you?

5. What topics would you like to see addressed in future videoconferences?

Return to: STARLINK, 9596 Walnut St., Dallas, TX 75243.