Chapter 7
Campuswide Security Education and Awareness
Shirley Payne

Computer and Network Security in Higher Education
Mark Luker and Rodney Petersen, Editors

A Publication of EDUCAUSE
The old adage “ignorance is bliss” does not hold up where IT security is concerned. To appreciate this, just listen in as a help desk staffer tells a tearful student that the only copy of his term paper (due that day) has been trashed by a computer virus and is unrecoverable. Or find yourself on the pointy end of the boss’s edict that you, a technically challenged human resources manager, will be held personally accountable henceforth for all security breaches in your department.

The need has never been greater for individuals at all levels and across all segments of the institution to understand what security threats exist and what to do about them. But how do you develop an effective education and awareness program for a topic that is not considered to be particularly interesting by the average person? How can you help such wide and varied groups of people on your campus (including students, parents, campus administrators, and the faculty, to name just a few) to understand the role they play in campus security? In this chapter, I examine some approaches to developing security education and awareness programs by defining target audiences and their unique needs for information, discussing a variety of techniques and tips for delivering the information to each audience, and suggesting strategies you can use for continuous improvement of your institution’s programs.
The Case for Security Education

First, let’s talk about why a security education and awareness program is so important—even when putting it together takes a lot of time and energy. Experts generally agree that people are the greatest source of IT security problems. Statistics consistently show that the majority of security breaches are caused by insiders, and the damage they levy on their organizations can be much more severe than anything wrought by hackers on the other side of the world (Pescatore, 2002).

Many, if not most, insider breaches are caused neither by disgruntled employees nor by students intent on doing harm. The sources are often people who either

- Are not aware of the security threats
- Are wrongly relying on someone else to deal with them
- Are not adequately skilled to address them, or
- Simply feel they have more important things to do

Unfortunately, potential intruders are all too aware of this human vulnerability, and they take advantage of it in a big way. Higher education offers many examples of security incidents leading to confiscation of hardware by federal authorities, loss or corruption of critical research data, and worse. Some have garnered national attention, and most could have been prevented with better education. Education, though, can be devilishly hard to deliver when

- Few computer users acknowledge personal responsibility for security
- Many consider the issue too technically complex for them to understand
• Executive and middle managers often fail to comprehend the business implications of poor security and consequently don’t assign it a high priority

• Security budgets and staff are typically stretched to the limit

In the face of these obstacles, it is especially important that a security education and awareness program be finely focused and all possible resources be leveraged. So let’s start by analyzing precisely what information needs to be conveyed, and to whom.

Target Audiences Within the Institution

The most critical messages and the most effective ways to convey them can vary greatly from one target audience to another. In many ways security education is a marketing campaign, and certain marketing principles apply: know the customers’ needs, select the right products for them, tailor the sales method for each customer group, monitor sales results, and repackage the product if needed. The customers to consider typically include the groups discussed next.

Administration

Because boards of trustees, presidents, vice presidents, provosts, department heads, and deans define strategic direction, set priorities, and allocate resources, an education and awareness program is necessary to help them understand security threats to the institution, risks posed by these threats, and what can be done to mitigate unacceptable risks. When security is explained in familiar business terms, it sheds its technical mystique, and managers at all levels can understand where to place it in the overall picture of operating the institution.

Along with providing a business case for security, a program should establish the right expectations among managers. They
must know that other institutions and industries have the same issues and that no organization can be 100 percent secure—despite all best efforts, new threats will continue to surface and will require new measures.

**Students and Parents**

Unless a mandate is enforced to configure all PCs alike, students will arrive on campus with a hodgepodge of computer brands, operating systems, and software applications. Few of these computers will be secure; when plugged into the institution’s high-bandwidth network, some will be victimized by crackers literally within minutes. It is important, therefore, to provide students with basic instructions for securing these computers before they arrive on campus. Involving parents in the education process can be helpful.

**Faculty and Staff**

This group can be a special challenge because faculty and staff typically believe it is someone else’s job to take care of security. Defining how security issues can affect them personally, outlining the specific steps they can take to prevent problems, and emphasizing their individual responsibility to take those steps is an effective approach here. Remember to include information about federal and state laws governing use and protection of data, such as the Family Educational Rights and Privacy Act. Staff will typically comply once they understand what is required of them. Faculty can best be reached by convincing them that safe computing won’t detract from their work—but unsafe computing surely will.

**Researchers**

Research labs are happy hacker hunting grounds. Security breaches are frequent, yet grant proposals that include the need for superpowered servers and workstations continue to leave unaddressed the need for knowledgeable system administration. Hence, this critical job often falls to underskilled (and sometimes unskilled) graduate
students. Educate researchers before they write proposals, clearly communicating what security measures are necessary and what the institution’s overhead allotment for research allows them to contribute, if anything, to addressing these measures. Include managers and staff from sponsored program offices in this education campaign.

**Health Care Professionals**

The administrative computing environments of teaching hospitals are commonly more centrally controlled than is typical of university academic computing. Desktop operating systems and applications are likely to be locked down—hopefully in a secure manner—with servers administered by central IT staff. Education on basic security steps, such as keeping operating systems up to date, may be less important here; but providing guidelines for handling sensitive patient data is paramount. Always an important issue, this is now even more critical as new federal Health Insurance Portability and Accountability Act (HIPAA) regulations become law. Penalties for noncompliance are significant for hospitals as well as for individuals. HIPAA regulations require ongoing education programs that address sensitive data security and accountability.

**Auditors, Campus Police, and Attorneys**

The wise security director recognizes the importance of working arm in arm with the institution’s internal auditors on many security strategies. The relationship can be effective, though, only if auditors fully understand IT security threats, risks, and appropriate remediation steps. Further, educating them on existing network-level security measures for the entire institution provides them with the broader context they need when auditing individual department situations.

Campus police are being faced more and more often with the need to investigate computer-related incidents. Like auditors, police assigned to these cases need a foundation of knowledge regarding threats and risks. They also must be familiar with cyber security law
and must be aware of resources, such as computer logs, that are available to help them with investigations.

In-house attorneys can help with several aspects of the security program, such as policy development. Also, executive management often calls on them for advice on IT security and responsible use issues. Again, ensuring that these individuals have a good understanding of threats, risks, and steps being taken to reduce risks is helpful.

State and Federal Government Relations Staff

The trend toward newer, tougher state and federal security legislation may provide important levers to aid higher education in addressing security problems, but it could also require actions that run counter to institutional culture and missions. Public schools that are subject to close oversight by state government are especially vulnerable. Individuals charged with responsibility for government relations must be alerted to possible new regulations and their potential impact on the institution, so they can exert favorable influence on proposed legislation.

IT Staff

There is no aspect of IT work that doesn’t concern security in some way. Computer account management, help desk support, database management, application development, network administration—all must be conducted with security in mind. People performing these duties must master security basics, and each must acquire additional knowledge relevant to his or her particular responsibilities. A security education program is not complete unless it addresses both the basic and the special training needs of technical staff.

Perhaps no group is in greater need of specialized attention than system administrators, who by virtue of their responsibilities can either foster or foil institutional security measures. These people almost universally desire to perform their functions in a secure manner; they just need to be shown how.
A wealth of specialized training materials and Web-based resources are available specifically targeted at IT staff members, and these should be incorporated into any security training program for this group of individuals. For example, the SANS (System Administration, Audit, Network, Security) Institute provides security professionals, auditors, system administrators, and network administrators with resources, such as news digests, research summaries, security alerts, and in-person and online training and certification programs (www.sans.org).

Similarly, the CERT Coordination Center at Carnegie Mellon University’s Software Engineering Institute provides training and education for technical staff and management on topics such as creating and managing security incident response teams, improving network security, and responding to and analyzing incidents (www.cert.org).

Effective Delivery Methods

Definition of customer groups simplifies the next important tasks: tailoring the security message for each group, and selling it effectively.

Meeting Presentations and One-on-One Discussions

Perhaps the most effective, albeit labor-intensive, means of building security knowledge is simply to custom-tailor presentations to specific groups and individuals throughout the institution. Doing so provides the opportunity to address specific questions to a captive audience. In one-on-one discussions with executives, it’s possible to place security issues in precisely the right context and to highlight key security concerns within each executive’s purview.

Handbooks

Security handbooks can be used to introduce students, faculty, and staff to security concerns and their responsibilities for addressing those concerns. Handbooks can be provided in hardcopy to all
new entering students and employees as part of their orientation programs, with electronic versions posted on the Web for ongoing reference.

**Online Quizzes**

Some institutions require that students and employees successfully complete an online quiz before receiving their computer accounts. The use of online quizzes can thereby encourage users to read their handbooks and can serve to highlight critical points. A quiz can also provide the means for formally capturing student and employee agreements to abide by the policies and procedures detailed in the handbook.

**Security Web Site and Web Ads**

The need to update information on security threats and countermeasures is constant, and the Web is an easy and inexpensive means of keeping this information fresh, as well as accessible. Most institutions provide some security materials on the Web, but this information is sometimes scattered across many Web pages, making it difficult to find. A security Web site acts as a clearinghouse for all security-related information, placing it at the fingertips of those who need it.

An effective technique for leading readers quickly to information most relevant to them is to organize the material by roles. A system administrator, for example, might be presented with one set of materials, an average desktop computer user with another, and a department head with yet another. A role-based security Web site also forces the designer to think about the unique needs of each target audience, which will help to more easily identify content gaps.

The Web can be leveraged in other ways as well. Web ads (not the pop-up kind, please) that promote tips for enhancing security can be quite effective when placed on well-traveled sites throughout the institution’s Web space.
Security Alerts

Information about the latest viruses and worms should be incorporated into the security Web site. Given how quickly these destructive programs can spread, though, it is also useful to push virus and worm alerts out to the user community. Existing mail lists of willing recipients can be used to e-mail these alerts or a new subscribed mail list can be set up for this purpose. Alerts might also be posted to the institution’s Internet newsgroups, and if the virus or worm is particularly nefarious, an alert posted on the institution’s home page may be appropriate.

A challenge with alerts is to maintain the level of customer interest. Too many alerts, and people tune them out; too verbose, and people don’t have time for them. Alerts should be used sparingly, be timely, convey only essential information, and eschew technical details.

Security Fairs, Conferences, Seminars, and Workshops

Shoeorning security information into preexisting events, such as new student orientations, is a relatively easy way to promote the topic. Events specifically focused on security, though, allow outreach to groups and individuals that might not otherwise be touched. A security fair that is co-located with a student dining hall, for instance, can provide good visibility among this busy group of users. Security conferences featuring high-profile speakers can draw faculty, administrative and IT staff, campus police, and others. Workshops on basic security topics are especially effective and appreciated by those motivated to learn more. And advanced technical seminars and workshops specifically aimed at system administrators and other IT staff are essential to every security education program.

Articles

Articles in popular institutional publications are perfect vessels for carrying security information out to people who would not ordinarily encounter it. With the federal government’s Department of Homeland Security enjoying so much press coverage, editors will
understand that general security is a timely topic, and the idea of highlighting cyber security can be quite appealing. They might even be convinced to devote an entire issue to the topic.

Handouts
Postcards and brochures that convey specific warnings and tips are inexpensive to produce in-house and can be used in a variety of settings, such as back-to-school events, new employee orientation sessions, and open houses. Handouts should be easy to carry, attention grabbing, and short.

Videos
A few institutions have used videos to draw attention to security issues. One uses a scenario format featuring two students talking about security. Another uses children to lampoon irresponsible computing behaviors. Given the number of issues that compete for attention with busy students and employees, videos that are brief and entertaining are an effective way to bring security into focus. These videos can be showcased at various events and piped to dorms and other locations via campus cable channels.

Security Topic in Broader Subject Courses
Incorporating the security topic into various preexisting courses is another effective strategy. A security component included in technical courses is almost always appropriate, but it also fits well into courses designed to train staff on administrative applications. As part of the training, it’s a good practice to require staff to acknowledge formally, perhaps via a signed memo of understanding, their responsibilities for protecting data obtained through the use of administrative systems.

Communication Tips
Security is a hard sell. Let’s review some techniques for serving up security information in a dish that’s palatable to customers.
• *Take the message to the people.* If you wait for your audience to come to you, you’ll be waiting a long time. Deliver the security message aggressively; use conventional means such as posters and handouts, but don’t neglect mechanisms such as bus placards, local TV and radio talk shows, and newspaper promos.

• *Be consistent in the message.* Everyone engaged in delivering security education should speak with one voice. Package the content and delivery for varied audiences, but provide the same fundamental message.

• *Write to short attention spans.* Wherever possible, break the message into small bits. If an idea can’t be conveyed in less than fifty words, it is too long. If you need to present six ideas, six postcards or Web ads are better than one long think piece.

• *Make the message real to each target audience.* All materials should reinforce the idea that “it could happen to you.” Use scenarios and case histories that are realistic and interesting for the particular target audience.

• *Make it fun.* Humor can be really effective when it is done well.

• *Repeat, repeat, repeat.* Use different angles to restate the most important pieces of the message in multiple ways.

**Keys to an Effective Education Program**

Security education and awareness programs must be updated continually to keep pace with emerging threats. Even the sharpest campaigns eventually lose their effectiveness. Strive to maintain value and interest in your program by applying new approaches and resources.
Solicit Input in Determining Priorities

A security education and awareness program can cover all of the basics and still not get the biggest bang for the buck. Comparing the program content to a prioritized list of high-risk security areas may reveal significant gaps. For example, most research universities recognize security lapses in their research projects, but their education and awareness programs may not include specific advice for principal investigators. Soliciting input from departmental system administrators and their bosses—asking what would help them the most in securing the computing environments they manage—can yield a better understanding of needed program improvements. Help desk staff and internal auditors can also provide valuable guidance for future development, since they see security vulnerability almost every day.

Base Program on Strong, Clear Policies

Building an education and awareness program can highlight policy lacunae. Advice to “Do this” or “Do that” usually begs the questions “Why?” and “What happens if I don’t?” Without good explanations and sanctions behind the advice, a program can go only so far toward changing undesirable behaviors. Strengthening a program may, therefore, require updating existing policies or introducing new policies that support what the program is trying to accomplish. It may also require obtaining the support of the most senior executives of an institution to make the policy stick.

Given the wide variation in policy implementations within our institutions, policies related to security may be found in other policy statements about acceptable use, computing and networking, or data administration, or they may be part of more discreet departmental policies. In any case, policies that deal with security should be robust and enforceable, and they should be clear about what actions are necessary on the part of the members of the community and why. When people understand that they are accountable, they are more apt to listen when told how to discharge their duties.
Good models exist for campus IT security policies, and many are available at the Web site for the EDUCAUSE/Cornell Institute for Computer Policy and Law (www.educause.edu/ICPL).

**Tap Creative Talents Throughout the Institution**

Education and awareness programs are likely to be powered mostly by central IT. Although technical staff must define the message, the talents of nontechnical people throughout the institution can be used to frame and deliver it. Public relations and communications staff are wonderful sources for new ideas, as are employees and graduate students who work in instructional technology and other fields. Media services within the institution, such as video production, may also be put to work for the program—if not for free, at least at a cost below that of commercial services.

**Place IT Security in the Context of Broader Security and Personal Safety Issues**

Although many people are fuzzy about the risks of cyberspace, they understand what it means to be generally secure and safe. Placing cyber security in the context of overall safety removes the mystique and disinterest usually associated with cyber security alone. Engaging the campus police in designing and conducting parts of your program helps tremendously to reinforce this notion, and allows police to leverage the program for their own education campaigns. Several institutions are doing this effectively today. The University of Maryland’s Department of Public Safety, for example, routinely includes information about computer security, spam, laptop theft, and related subjects in its regular newsletters. Campus police departments at many other institutions devote entire sections of their Web sites to safety in cyberspace and include practical advice on topics such as scams, stalkers, viruses, and hoaxes. (For an example, see www.ou.edu/oupd/inetmenu.htm.)
Consider Outreach Beyond the Institution

Once a program is in place and functioning well, there is the opportunity (and arguably an obligation) to take your message beyond the walls of the institution to local citizens, police departments, local and state governments, K–12 institutions, and businesses. Addressing these target audiences will almost surely bring new issues and perspectives into focus for the institution, and these can be used to enrich the program in ways that benefit all.

Build Partnerships Within and Outside the Institution

In addition to campus police, other organizations in the institution may serve as allies. If the university has a teaching hospital, partnerships with offices there are likely to be essential. Federal HIPAA regulations mentioned earlier will not only exert a major impact on health care workers, but will also affect people throughout the institution who work with protected health information. Student health staff, employee counseling staff, and research teams are a few examples. A partnership between the academic and medical sides of the house will help ensure that these people receive consistent education that addresses broad security issues and HIPAA in a single package.

Consider partnerships with other entities as well. With cyber stalking generally on the rise, for instance, women's centers may wish to participate in your program to educate students and employees on the topic. Student organizations may also show interest.

Alliances outside the institution may also be feasible. Consider partnerships in which the school already participates, such as those with vendors, other schools, government entities, and professional associations. The University of Virginia, for example, partners with the Federal Bureau of Investigation (FBI) to operate the FBI Academy, which offers criminal justice education programs (www.scps.virginia.edu/departments/fbi.php). This institution was able to capitalize on the relationship to obtain field-experienced faculty to teach a computer forensics class to staff.
Leverage What Others Are Doing

Finally, programs can get a significant boost by taking advantage of what others are doing successfully. Higher education institutions enjoy a long tradition of sharing among themselves, and in the realm of security education and awareness, what works well for one will probably work well for another. For example, the Virginia Alliance for Secure Computing and Networking (vascan.org) was formed by four universities (George Mason University, James Madison University, the University of Virginia, and Virginia Polytechnic Institute and State University) to share their security tools, best practices, and services (including education and awareness programs) with others in that state. EDUCAUSE provides similar resources at the national level through the EDUCAUSE/Internet2 Computer and Network Security Task Force (see www.educause.edu/security).

U.S. government-provided information is another resource to tap. The recently formed U.S. Department of Homeland Security (www.dhs.gov/dhspublic) is expected to yield additional tools and best practices, and the National Institute for Standards and Technology Security Resource Center (csrc.nist.gov/ATE) has long offered awareness, training, and education guidelines.

University-based security research centers are also good sources for courses and educational material. Purdue University’s Center for Education and Research in Information Assurance and Security (CERIAS; www.cerias.purdue.edu), for example, is a leading provider of excellent courses and resource material for a variety of audiences, including K–12 and home users. CERIAS also has an active research program that covers a wide range of security and information assurance topics, as well as a continuing education program for postsecondary education.

Conclusion

The techniques described in this chapter cannot alone resolve all security concerns on campus but must be an integral part of an
overall plan for security that involves specific technical approaches, policy development, and education programs. Even the most effective education and awareness program can only enable us to stay abreast of new threats and to exercise due diligence in making computer users aware of them. Even this much, though, is critical. Given the rapid and continuous growth of cyber threats to our institutions, we can afford nothing less than a security education and awareness regimen that is persistent, pervasive, and compelling. To borrow from a popular bumper sticker: If you think education is expensive, try ignorance.

Reference