College-Level Education for Cyber Security

Jay Corzine

Colleges and universities provide an additional venue for the delivery of educational programs to enhance both individual and institutional levels of cyber security for a large cross-section of the younger population. A significant percentage of graduating high schools seniors enter a college or university within 4 years of completing high school. Besides the provision of a useful service for their student populations, colleges and universities have an enlightened self-interest in enhancing the cyber security literacy of their undergraduate students. The contemporary university is "wired" and highly dependent on the operation of complex computer networks for teaching, research, and management functions. Each fall semester, dependent on its size, a college admits several hundred to several thousand first-year students who will almost immediately be granted access to university email accounts and online systems for browsing library holdings, monitoring student records, completing course assignments, and so on. Similarly, higher education must take steps to limit the incidence of illegal downloads by students. Simply stated, it is in the best interest of the colleges and universities to provide mandatory education that will decrease the risk of students infecting computer systems with viruses, worms, and spyware. Programs that impart knowledge designed to protect the university's networks can also be used to convey information that will lower students' risk of identity theft and other cybercrimes that target individuals.

Although education to increase individuals' cyber security is necessary for students in the K-12 system, there is an important added risk for becoming a cybercrime victim when individuals become legal adults at the age of 18, namely the credit card. . The stuffing of mail boxes with credit card offers coincides with the entry of traditional-age college students into institutions of higher education and is widely supported by colleges and universities through their selling of student lists to companies hawking credit card companies as well as a laundry list of others products and services. In fact, some universities sell the excusive right for a credit card company to distribute application forms on their campuses. The possession of one or more credit cards increases the risk of being a victim of frauds perpetrated through computers, and it can be argued that colleges and universities who facilitate their acquisition by student have a moral obligation to provide education to reduce the risk. One innovative approach would be for institutions of higher education to require credit card companies to provide cyber-security education, perhaps in an online format, to students prior to the issuing of a credit card or forego access to student lists.

Cyber security for incoming first-year students can easily be introduced through the new student orientations that are increasingly required by most large state universities prior to enrollment for courses. Typically one-to-two day events structured to introduce the student to the campus and

complete bureaucratic paper work, most colleges and universities have sufficient flexibility in orientation schedules to require attendance at a 30 minute segment on cyber security. Although some time can be devoted to reinforcing strategies to protect against viruses and worms, precautions that were hopefully part of students' K-12 education, attention should also be focused on identity theft, including phishing and pharming. The information can be provided through lecture and/or videotape format with some provision for a Q&A period. In fact, some universities have moved in this direction. Many colleges now include short 15 – 20 video presentations on cyber security often produced by its computer security technology departments as part of its orientation sessions for new students. Including cyber security as a topic in student orientations has the advantage of reaching all incoming students before they have access to university computer systems.

An alternative to including cyber-security education as part of orientation would be to require the completion of a training program before allowing students to obtain a university computer account. This would allow for a more comprehensive package of information that could be delivered in an online format and would be a reasonable alternative for colleges and schools that do not require students to complete an orientation program. An additional advantage is that a sequence of training programs could be developed with the specific requirements tied to the type of accounts desired by a student. In order for information on individual cyber security to be widely disseminated, there would have to be an introductory-level training module required for all students, however. The completion of the base module could be tied to the issuance of a student ID.

To attain a higher level of national cyber security, it is vital that higher education closely examine the content of introductory courses in computer science programs. Presently, these courses rarely include material relevant to cyber security. Although not all students take these courses, they are increasingly a mandatory or elective requirement for general education programs and enroll a significant percentage of undergraduates in many colleges and universities. They would provide a forum for more detailed readings and discussion focused on cyber security, and it is reasonable to expect that in schools where they are elective, these courses enroll those students who are likely to both have a greater interest in and to make more use of computers. These courses would be a logical place to cover precautions directly tied to network security, a growing concern for all organizations, including colleges and universities.

Of course, there are two primary limitations to an over reliance on colleges and universities to provide education about cybercrime and cyber security. First, not all people attend institutions of higher education. Second, and perhaps more importantly, the risk of victimization from some types of cybercrime, e.g., cyber stalking, occurs prior to high school graduation. But colleges and universities can provide an important part of a comprehensive, national educational

program designed to reduce cybercrime victimization.