COMPUTER SECURITY
TRAINING AND EDUCATION:
A NEEDS ANALYSIS

Stephen F. Barnett
Deputy Director
National Computer Security Center
sbarnett@romulus.ncsc.mil

Abstract

This position paper examines, from an employer’s perspective, the kind of education and training today’s computer security practitioners need. It suggests answers to three important questions: What are we educating people to do? What should be included in education and training programs? What can industry do to help?

1. What are we educating people to do?

Because computer security knowledge, skills and abilities are applied in a variety of work environments, training and education programs have to prepare students for different kinds of jobs. Broadly speaking, one can categorize these as jobs in which one is (a) dealing with pragmatic, operational issues, via the front line troops doing system administration, system management, decision making and policy development; or (b) providing technically sound solutions for computer security needs through research; countermeasure design, development, test and evaluation; and integration of countermeasures into system solutions. The education and training needs of people working in these two areas is very different with respect to content, breadth and technology used. The former are dealing with real time operation of computer hardware and software which may be newly released or many years old. People in operational computer security must be prepared to characterize and manage security risk with respect to their systems. They must understand why the procedures and practices need to be followed. They must understand what risks their systems are facing, be able to detect and analyze anomalous conditions and make decisions about corrective action. Those working in computer security technology are dealing with the most recent releases of computer hardware and software and, in anticipation of new technology and advances in the threat, are developing new techniques for strengthening computer defenses. By characterizing current and future risk, their work leads to providing state-of-the art security techniques and products.

We are educating people to work with networked systems in which local events can have global security consequences, and global events can have local security consequences. Thus, they must understand the implications of connecting computers to networks and protecting information as it traverses the network, as well as protecting information systems from attack via the network.

Finally, we are educating people to do computer security not as “another assigned duty”, but as a career path unto itself, in a field which is changing as rapidly as the underlying information system technology. Thus, people must get education and training foundations to enable them to work effectively in a variety of situations, and to stay current with both information system technology and advances in computer security threat, tools, techniques, solutions, and risk containment. Those dealing with operational situations need breadth of knowledge, and the skill to apply it on the particular kind of systems they are working with. They must be able to apply their knowledge and skills to new information systems as the old systems are replaced. Those doing technology development need a broad understanding of the fundamental issues and technologies, but are more likely to need or develop knowledge in a more narrowly focussed aspect of the problem. However, since the underlying technology can change so quickly, yesterday’s most popular problem and solution may be of no use tomorrow. So technologists need to be educated broadly enough to allow them to move rapidly to new problem areas and new technologies.

2. What should be included in education and training programs?

The foundation of any computer security education or training should provide the student with the motivation for the field, i.e. why do we worry about computer security, why is there a problem, and what are the potential consequences? There should be a discussion of underlying principles for designing, building, testing, installing and operating computer
security countermeasures. These principles have been developed over the last thirty years and are variously enunciated in the literature and published standards and criteria. Students should be taught about threat and vulnerability, using case studies whenever possible, and giving them hands on experience. But the focus of the education and training program should be the more challenging problem of how to detect and obviate attacks, not how to perpetrate them. Students should learn about the major technologies for protecting systems, e.g. identification and authentication, secure operating systems, audit techniques, cryptography and other network security mechanisms. This foundation training ought to provide the student with knowledge of tools and techniques to characterize and manage risk.

The program should allow the student to build upon this core training according to their interests and career goals. For example, those wishing to work in operational computer security might receive training in threat assessment; and on effective use of tools for system security administration, on-line security testing, incident investigation, and risk management. Those pursuing careers in computer security technology development might receive advanced education and training in areas such as software design methods; system security engineering; secure operating system design, development and testing; design and application of network security techniques; or design and development of tools for performing security audits, testing or incident investigation.

As with any other academic discipline, this material should not be conveyed in isolated courses. Rather there should be a well defined curriculum of courses covering these topics at the introductory, intermediate and advanced levels so that students can choose a path through the curriculum to receive the depth and breadth of education suited to their needs and background. Because of dependencies between these topics, some courses would undoubtedly be prerequisites for others. Tailored versions of these courses ought to be available to students in fields in which computer security is a major concern in the work environment, for example business administration, public administration, or finance and accounting. By infusing security training in these curricula, students are taught to make good computer security practices part of their job.

Finally, there is a lot of prerequisite knowledge that a computer security student must have regardless of whether they are preparing for a career in operational computer security or in computer security technology. They should know to some appropriate level the underlying technology; computer hardware and software terminology, architecture and design principles; networking hardware and software terminology, architecture and design principles; communication protocol design and operation.

Computer security education and training should not be treated as an abstract academic discipline. Formal classroom instruction should be augmented with case study analysis, student projects to teach analytic and technical skills, and work on hard, possibly unsolved problems in computer security design, evaluation, engineering, or operation. By so doing, students are better prepared to deal with actual tasks when they enter the work place. Cooperative education programs between academic institutions and organizations employing computer security personnel is an option for combining academic training with on-the-job experience to build skills. Post employment training can teach the new employee about the employer’s policies, philosophies, practices and systems.

3. What can industry do to help?

Companies with an interest in computer security education can set up co-op programs for undergraduate students, and support graduate training in computer security for their employees. They can endow a computer security chair on the faculty of a university or create exchange programs in which employees join the faculty and teach for an academic year or lecture at specific courses. They can provide information about case studies or challenging problems for students to work on. Employers should allow computer security personnel time to give and get training (10-15%), to continue their education, and attend and participate in computer security conferences. Finally, computer security personnel should be given challenging assignments to continue to develop their skills and knowledge, and get recognition of good work. This latter is particularly important in system security administration which is becoming an increasingly critical and highly technical career field.