A Public Health Education Approach to Computer Security Education

Jane Jorgensen

Abstract— **The continued proliferation of crude and poorly disguised malware, such as those spread by execution of email attachments, has highlighted the failure of large-scale security education to convey simple messages such as "don't open email attachments sent by strangers." Computer security education, like public health education, is not a 'one-size-fits-all' endeavor. Needs, goals, and curricula to achieve these goals must be carefully assessed for the population targeted. Once the intervention has been delivered, its results must then be evaluated to assess the impact of the program. This paper describes a public health-based framework for needs assessment in security education.**

I. Public Health Perspective to Security Education

Public health professionals have acquired a wealth of experience in the use of health promotion and education programs to reduce morbidity and mortality in human populations. Security education programs focus on an analogous goal, the reduction of damage and loss due to malicious attacks on computers and computer networks. We examine techniques that can be used to extend this paradigm to the development of computer security education. The requirements for both are directly analogous. Both should convey information that has been deemed to be important in an evaluable manner to a clearly identified population. In the remainder of this paper, we discuss the way in which the public health framework might be applied to computer security education.

Specific issues to be addressed in the design, implementation and assessment of directed educational programs in general are shown in Table 1. These issues are routinely addressed by health educators as they plan health education campaigns.

The mission of public health is to "fulfill society's interest in assuring conditions in which people can be healthy" [1]. Health education programs use a combination of learning experiences that promote voluntary actions and informed decisions conducive to health to realize this goal.[1] These efforts consist of clearly identifiable components: identification and assessment of need; planning and implementation; and evaluation and communication of results.

II. Needs Assessment

Health education programs are designed to satisfy specific needs. There are many ways of ascertaining these needs, some of which are more subjective than others. McKillip [2] defined a need as " a value judgment that some group has a problem that can be solved." Needs are identified and examined through a process called needs assessment. There are several strategies for conducting needs assessment. For example, Basch [3] suggested that issues such as the following be used to determine need. (Questions addressing computer security are shown in parentheses.)

- Distribution (Whom does the problem affect?)
- Prevalence (How widespread is the problem?)
- Severity of consequences for individuals (How severe is local damage and loss?)
- Severity of consequences for community (How severe is network-wide damage and loss?)
- Urgency (How quickly is the problem expected to worsen?)

Identification of clearly identified target populations is an important part of needs assessment. In their Model of Community Analysis, Dignan and Carr [4] recommended that health educators identify (1) the

This work was sponsored by the Defense Advanced Research Projects Agency under Air Force Contract F30602-00-C-0020. The views, findings, interpretations, and conclusions are those of the authors and should not be construed as an official Department of Defense position, policy, or decision

The author is a Principal Scientist at Information Extraction and Transport, Inc., 1600 SW Western Blvd., Suite 300, Corvallis, OR 97330. The author's current email address is (jorgenj@camas.org).

[1] Many corporately sponsored health education campaigns appear to be no more than glorified advertisements. Such campaigns are designed to benefit the corporate bottom-line and to generate sales. These are public relations efforts, not health education and promotion campaigns.

TABLE I
ISSUES TO BE ADDRESSED IN THE DESIGN, IMPLEMENTATION AND EVALUATION OF TARGETED EDUCATIONAL CAMPAIGNS

DESIGN
What is the problem to be addressed?
Who is affected by the problem? By the solution?
How severe is the problem?
How urgent is the problem? How much time can be allocated to the solution?
Are there any undesirable collateral effects?
Do the ends justify the means? (Is the program defensible?)
IMPLEMENTATION
What resources are available to solve the problem?
Are the results feasible? Measurable?
EVALUATION
How will the program be evaluated?
Were the objectives attained? Why or why not?

resources and needs of a community and (2) target populations, as a prelude to planning appropriate health education programs to meet the needs of a specific target population. McKillip [2], in his model for needs analysis, stressed the importance of obtaining the support of members of the target population, referring to them as 'customers'. He suggested that services and eligibility restrictions also be assessed and that the needs of the target population be prioritized and the results of the assessment be communicated to this population.

In a more comprehensive approach spanning planning, implementation and evaluation, Green [5] developed his PRECEDE (Predisposing, Reinforcing, and Enabling Causes in Educational Diagnosis and Evaluation) model, drawing from epidemiology, social/behavioral science, administration, and education. In a PRECEDE analysis, problems are prioritized and, where resources are limited, the most important problems with achievable results are addressed first. The components of a program performed using the PRECEDE model are listed below. (Parallel activities related to computer security issues are given in parentheses.)

- Social assessment (Identify problems in target population.)
- Epidemiological assessment (Assess damage and loss.)
- Behavioral assessment (Assess utilization patterns for system administration services, preventive security behaviors, compliance with security regimens.)
- Educational assessment (Identify factors that predispose, enable, or reinforce behavior; assess knowledge and attitudes about computer security.)
- Select appropriate educational materials (Develop curriculum for security issues.)
- Administrative (Examine feasibility and assess available resources for computer security programs.)
- Evaluation (Perform formative and summative evaluations.)

Evaluation is an integral part of an education program. Formative evaluations address the implementation process. Summative, or outcome evaluations contain outcome analyses.

III. SECURITY EDUCATION SCENARIOS

When we examine the range of potential security education efforts from a public health perspective, we can discern many target populations, needs, objectives and beneficiaries. We compare three notional education efforts directed towards developers, network administrators, and general users with respect to goals, curricula, and outcomes.

Computer security is an issue that concerns vendors and users. Although the importance of security may be widely accepted, the means for achieving it are not transparent. Graham Cluely, a senior technology consultant at Wakefield, Mass-based Sophos Anti-Virus, noted that "the Internet plays a dual role in this problem – it's the mechanism for the delivery of the viruses as well as for the cure, which has lulled some into apathy" [in 6].

A. Educating Developers

Pressure has been mounting on application developers to create secure software. Many applications are known to contain security holes and the burden has fallen to the user to maintain the security on individual computers and networks by downloading patches. Operating system software shipping with new computers must be patched upon receipt to rectify known vulnerabilities. Ron Ehlers, Vice President of Information Systems at Pacific Sunwear in Anaheim, CA has called attention to such vulnerable software: "The industry, so far, has taken the approach that everyone is kind of on their own and has to fix problems themselves whenever they arise. We need to see more attention paid to this by the vendors" [in 6]. The needs assessment conducted prior to this campaign might solicit opinions from stakeholders such as Charles Dulin, formerly of Internet Privacy Solutions, based in Hawthorne, NY: "What [application vendors] have been trying to do is push the liability back to the consumer and accepting none for themselves" [in 6]. Implementation might consist of a curriculum developed by one company or a consortium of companies addressing specific issues in the generation of secure application code. One measurable

outcome might be the reduction in the number of known vulnerabilities present in software shipped.

B. Educating Administrators

An educational campaign conducted by software vendors for their developers would be very different than other campaigns targeting system/network administrators or general users. An educational campaign benefiting an organization by targeting its system and network administrators would also contain a specialized curriculum. Such organizations might engage in these campaigns to reduce their exposure to risk by implementing documented security education programs. Jeremy Epstein, Director of Product Security at webMethods predicts that users as well as vendors will be held liable when security education is overlooked. "Customers who fail to protect and maintain their networks will be held responsible by their partners and customers for spreading security problems" [in 6]. Liability insurance may become a necessity, said Al Varrachio, Assistant Vice President of Kaye Tech Risk Solutions, a technology liability division of New York based insurance brokerage Kaye Group, as users are held liable for failure demonstrate due diligence in protecting their networks [in 6]. One cyber liability underwriter, Okemos, Mich-based J.S. Wurzler Underwriting Managers, has already introduced incentives and disincentives, increasing premiums by 5 to 15 percent if a user's MS Windows NT administrators are insufficiently trained. If administrators' training is current, clients are rewarded with a 20 percent discount [in 6].

In this type of educational campaign, the curriculum is targeted to system and network administrators and the information they need to protect their networks by maintaining security postures; detecting intrusions and infections in a timely manner; and restoring their systems and networks as soon as possible following a security breach. Evaluable outcomes might include the number of attempted intrusions intercepted, the number of scans and probes detected, the timeliness and completeness of security updates, and the time to partial and full recovery following an attack.

C. Educating the General Public

In our final scenario, we consider an educational campaign targeted to users in the general public. The number of Americans connected to the Internet has grown 63 percent in the past two years with three out of five Americans (58 percent) now connected to the Internet. Those using the World Wide Web spent an average of 10 hours and 19 minutes online during July 2001 alone [7].

Children form a significant segment of this group: 45 percent of American children (equal numbers of boys and girls) under the age of 18 go online (73 percent of those between 12 and 17 go online). These children engage in a wide range of tasks on line, often simultaneously emailing, instant messaging, surfing the Web, and for many who have access to an available phone line as well, talking on the phone, too. A study by the Pew Foundation [8] conducted interviews with teens who described experiences including the following:

- "I do so many things at once," acknowledged one 15-year-old girl in the Greenfield Online group discussion. "I'm always talking to people through instant messenger and then I'll be checking email or doing homework or playing games AND talking on the phone at the same time."
- "I get bored if it's not all going at once, because everything has gaps - waiting for someone to respond to an IM, waiting for a web site to come up, commercials on TV, etc."

The Internet is a social experience for these teens. According to the Pew Foundation report, 83 percent of the teens interviewed said they had gone online with a group of others around one computer. It was common for one group of teens to be instant messaging another group of teens at another computer. The level of activity was observed to increase from middle school to high school. While only a third of middle school students said that they used the Internet every day, this number rose to almost half for high school students [8].

The curriculum materials targeted to this group must incorporate this social aspect of Internet use to engage its target population. Directed learning activities might be accomplished in teams and adherence to security protocols could be couched in terms of extending the terms of friendly engagement. We must teach security educators to address the specific needs of this group.

Very simple explanations of how viruses and worms affect systems and how to disinfect systems might also be included in curriculum. The importance of antivirus protection and basic procedures for disinfection are also potentially valuable elements of the curriculum for this group. Also, school provides a convenient location for delivery of the curriculum.

IV. Defensibility of Programs

Health education campaigns, in addition to being necessary, must also be defensible. They should not create more problems than they solve. DL Stufflebeam *et al.* [9] asserted that to assess the defensibility of a program, its purpose must be clear. They suggested four criteria to justify defensibility:

TABLE II - TARGETS FOR THREE NOTIONAL SECURITY EDUCATION PROGRAMS AND THEIR BENEFICIARIES, FOCUS, GOALS, AND POSSIBLE OUTCOMES

TARGET	WHO CONDUCTS/BENEFITS?	CURRICULUM FOCUS	GOALS	MEASURABLE OUTCOMES
Developers	Software development Entity/users	Creation of secure software	Prevention	Number of incidents caused by defective software
Network, system administrators	Employer/ employer, users	Maintain operational systems & networks	Prevention, Detection, Maintenance, Recovery	Number of detected intrusions, length of recovery
Users	Public agencies (e.g., schools)/users, public-at-large	Avoid infection, disinfect promptly when infected	Prevention, Recovery	Smaller and shorter epidemics

- Proprietariness criterion: Are the rights of the individual preserved?
- Utility criterion: Is there a benefit to society?
- Feasibility criterion: Are the objectives achievable?
- Virtuosity criterion: Does the program foster excellence?

Using the criteria suggested by Stufflebeam *et al.* [9], a defensible program preserves the rights of the individual, possesses utility, and is both feasible and virtuous. Given that the goal of the educational campaigns is to promote voluntary actions and informed decisions conducive to health through learning experiences, we must determine that the curriculum contains useful, achievable, beneficial content that does not impinge on the rights of the individual. Programs not meeting these goals would provide trivial or overly complex information with no useful purpose, implemented in such a way that impinges on individual rights. An evaluation assessing the impact of the program that violated the rights of an individual, for example, by illegally monitoring email communications, would not be defensible.

V. ROLE OF CYBER EPIDEMIOLOGY

As we have discussed, any curriculum must be designed to deliver content in a way that will encourage recipients to make voluntary, informed decisions that decrease their risk of loss of information and damage to assets while engaged in activities using computers. The selection of issues to be addressed by the curriculum will be tailored to the needs determined by the needs assessment and prioritized based on the relative risk of the threat. However, the presentation of these risks can be problematic. The quantitative assessment of risk is a historically recent invention and colors our perception of the world. Skolbekken [10] refers to this as a "risk epidemic…. a social construction of a particular culture at a particular time in history."

The 'paradox of health' defined by Barsky [11] is that the perception of well-being and satisfaction with personal health in the United States have declined in the past few decades even though there has been a concomitant improvement in the collective health of the nation as a whole. In education, even though tools for health improvement may be provided to a target population, fear of disease continues to be a prime motivator. One side-effect of health education is that people are made more aware of the problem while they remain unconvinced about the efficacy of any solutions provided. A similar phenomenon in security education would preclude the popular perception of success for any program. Success then, becomes contingent upon achievement of clearly defined, evaluable objectives.

Lay epidemiology, the idiosyncratic interpretation of correlations to infer causation at a very local, common-sense level, also presents a barrier to the objective assessment of risk. The author has experienced this phenomenon first-hand, when a young acquaintance insisted that no disinfection of her infected computer was necessary because her email program would soon "run out of viruses to send." Information about risk must be presented in a balanced manner that induces changes in injurious behaviors without obstructing the way responsible people work, play, and communicate using computers.

The balance between the presentation of risk as an informative strategy to induce behavioral change and as a coercive strategy to demand change is a delicate one. Coercive risk awareness has been referred to as "a form of cultural imperialism" [12]. Beck [13] described our society as one in which people exhibit a heightened awareness and preoccupation with environmental risk. As these risks become apparent, the art of security education will be to preserve the innovation, freedom and power of computer-driven activities while maintaining adequate levels of security.

REFERENCES

[1] Institute of Medicine, Committee for the Study of the Future of Public Health, Division of Health Care Services, *The Future of Public Health*. Washington, DC: National Academy Press, 1988.

[2] J. McKillip., *Needs Analysis*. Beverly Hills, CA: Sage, 1987.
[3] C. E. Basch, "Assessing health education needs: A multidimensional-multimethod approach," in *Handbook of Health Education*, 2nd ed., P. M. Lazes and L. H. Kaplan, KA Gordon, Eds. Rockville, MD: Aspen, 1987.
[4] M. B. Dignan and P. A. Carr. *Program Planning for Education and Health Promotion*. Philadelphia: Lea & Febiger, 1987.
[5] L. W. Green, M. W. Kreuter, S. G. Deeds and K. B. Partridge. *Health Education Planning: A Diagnostic Approach*. Palo Alto, CA: Mayfield,. 1980.
[6] B. Fonesca and T. Sullivan. (2001, August 14). "Persistent viruses sound industry alarm." CNN [Online]. Available: http://www.cnn.com
[7] M. Mosquera. (2001, August 13). "Three out of five Americans connected to net." *InternetWeek* [Online]. Available: http://www.internetwk.com
[8] Pew Research Center. (2001, 20 June). "Teenage Life Online: The Rise of the Instant-Message Generation and the Internet's Impact on Friendships and Family Relationships." {Online]. Available: http://www.pewinternet.org
[9] D. L. Stufflebeam, C.H. McCormick, R.O. Brinkerhoff and C.O. Nelson. *Conducting Educational Needs Assessments*. Boston, MA: Kluwer-Nijhoff, 1985.
[10] J.-A. Skolbekken. "The risk epidemic in medical journals," *Social Science Medicine*, vol. 40, pp. 291-305, 1995.
[11] A. J. Barsky. "The paradox of health," *New England Journal of Medicine*, vol. 318, pp. 414-418, 1988.
[12] O. H. Forde. "Is imposing risk awareness cultural imperialism," *Social Science Medicine*, vol. 47, pp. 115-1159, 1998.
[13] U. Beck. *Risk Society: Towards a New Modernity*. London: Sage, 1992.