Herding Grasshoppers
September, 2003
Rebecca Herold, CISM, CISSP, CISA, FLMI
First published in the November 2003 CSI Alert Newsletter

Teaching should be such that what is offered is perceived as a valuable gift and not as a hard duty --Albert Einstein

I enjoy walking through my hay fields in late August. The grasshoppers are large and numerous in the late summer heat and dryness…they all hop out of way like green popping corn as I walk through the knee-high grass. I have a great feeling of control over the grasshoppers' movement; I can direct when they hop, where they hop, and they seem to be following my wishes based upon my actions. However, if I pause and look back, I will see them all hopping right back to where they were, continuing on their original path and doing what they were doing before, only temporarily detoured by my influence. I really didn't have the effect it initially appeared I had on these seemingly amenable creatures. Without my constant intervention and revisiting, they will always go right back to what they were doing before I disturbed their pastoral dining.

This parallels the typical effects of a security and privacy awareness and training program. It may appear you are in control of the education situation. However, if you do not remain diligent in your efforts, and constantly look back to reevaluate your effectiveness and modify your activities accordingly, it's likely the grasshoppers in your organization have hopped back to their old, familiar ways.

Awareness and Training Needs
Privacy and security awareness and training are important activities and key components of an effective privacy and security program. In fact, many regulations require awareness and training as part of compliance. The most commonly discussed right now are HIPAA, Sarbanes-Oxley (SOX) and GLBA. However, personnel education has been a requirement under other guidelines and regulations for several years. For instance, the Federal Sentencing Guidelines, enacted in 1991, and often used to determine fines and restitution for convictions, have seven requirements, one of which is for executive management to educate and effectively communicate to their employees the proper business practices with which personnel must comply. Issues that impact the severity of the judgments include consideration of the following:

- How frequently and how well does the organization communicate its policies to personnel?
- Are personnel effectively getting trained and receiving awareness?
- What methods does the organization use for such communications?
- Does the organization verify the desired results from training occur?
- Does the organization update the education program to improve communications, and to get the right message out to personnel?
- Does the training cover ethical work practices?
- Is there ongoing compliance and ethics dialogue between staff and management?
- Is management getting the same educational messages as the staff?

Sentences under the Guidelines can go up to $290 million plus jail time, or even higher in some circumstances.   But, are these guidelines really ever used? The U.S. Sentencing Commission documents that in 1995, 111 organizational defendants were sentenced according to the Guidelines, with 83 cases receiving associated fines. By 2001, the number of organizational defendants sentenced rose to 238, with 137 getting fines and 49 getting both fines and restitution. The average fine was $2.2 million and the average amount of restitution awarded was $3.3 million. 90 of those sentenced had no compliance program, which was a documented culpability factor in the sentencing. Having a poor compliance program was also a documented factor in other decisions.

Just a few of the other regulations besides HIPAA, GLBA and SOX that have awareness and training requirements include:

- 21 CFR Part 11
- Bank Protection Act
- Computer Security Act
- Computer Fraud and Abuse Act
- Privacy Act
- Freedom of Information Act (FOIA)
- Federal Information Security Management Act (FISMA)
- Digital Millennium Copyright Act (DMCA)
- DOT HM-232
- And so on…

Much has been written about the need for security and privacy education through effective awareness and training activities. A regulatory education program should address your organization's interpretation of applicable privacy and security laws and regulations as well as support the activities your organization will take to mitigate risk and ensure security and privacy. It is vital for organizations to evaluate, and continue to reevaluate, the effectiveness of these education programs. I have seen too many organizations spend considerable time and money to launch awareness and training programs only to let them then wane, wither and die on the vine because they did nothing beyond the big implementation; they failed to put forth the effort and activities necessary to evaluate, update and modify their programs as necessary to be truly effective.

Evaluation Areas
The methods you use for evaluation and measurements are diverse. The following objects of evaluation identified by Verduin and Clark (John R. Verduin, Jr. and Thomas A. Clark. Distance Learning. San Francisco: Jossey Bass, 1991) are useful. Tailor them to facilitate the evaluation of your organizational education programs by considering the questions listed with each object.

1. **Access.** What groups are you reaching? Are there groups missing? Is everyone in the target group participating? Are you providing appropriate delivery methods for your target audiences? Can all your target audience access your training and awareness materials and participate in your delivery methods?
2. **Relevancy.** Is your education program relevant to your organization's business goals and expectations? Are your training and awareness messages and information relevant to job responsibilities? Will your education program have a noticeable impact on business practices? Was your training content appropriate for your target participants? Did your training cover regulatory and policy requirements?
3. **Quality.** Is the quality of your awareness materials adequate to get attention and effectively deliver the intended message? Does the quality of your training materials contribute to your students' success? Do your trainers and teachers deliver quality education? Do they know how to interactively adjust to the abilities and experiences of their students? Were the conditions right for learning and for each learner's subjective satisfaction?
4. **Learning Outcomes.** Is the amount of time allowed for learning appropriate for successfully understanding the message? What do your participants say about the usefulness and effectiveness of your training and awareness activities? Do you tell the participants the expected outcomes of your education activities?   What did the participants actually learn? Did your participants indicate they had a satisfactory learning experience?
5. **Impact.** What is the impact of your education program on your organization as a whole? Were activities and habits changed appropriately following training and awareness activities? What are the long-term impacts? Did the training methods promote the desired skills? Did job performance improve? What is the pattern of student outcomes following each training session? Did you assist managers with determining their own workforce performance? Did you create return on investment statistics to support training and awareness funds?

6. **Cost Effectiveness.** What time requirements are involved? What are the costs for the materials? How many people are in your targeted groups? How is training being delivered? Are you using inside and/or outside training and awareness resources? What is the value of the method of awareness activity or training session you used compared to other awareness and training options?
7. **Knowledge Generation.** Do you understand what is important for your personnel to know? For your managers to know? Do you understand what works and what doesn't work in your education program? Are you utilizing your evaluation results? Did you assist employees in determining their own performance success? Did you compile trend data to assist instructors in improving both learning and teaching?
8. **General to Specific.** Do your instructors tell students enough information to allow them to self-evaluate their own success in implementing what they learn? Are students told overall goals and the specific actions necessary to achieve them? Are goals and actions realistic and relevant? What is the necessary prerequisite general and specific knowledge?

Evaluation Methods

Consider using a combination of the following methods for determining the effectiveness of privacy and security education within your organization. Be sure to discuss the methods with your legal department prior to implementation to make sure you are not violating any applicable laws, labor union requirements, or employee policies.

1. Videotape your training sessions. Review and critique to identify where you can improve delivery, content, organization, and so on.
2. Give quizzes immediately following training to measure comprehension.
3. Distribute a privacy and security awareness survey to all personnel, or to a representative sample. Do this prior to training to establish a baseline, then following training to help determine training effectiveness.
4. Send follow-up questionnaires to people who have attended formal training approximately four to six months following the training to determine how well they have retained the information presented.
5. Monitor the number of compliance infractions for each issue for which you provide training. Is this number decreasing or increasing?
6. Measure privacy and security knowledge as part of yearly job performance appraisals.
7. Place feedback and suggestion forms on an appropriate intranet web site.
8. Track the number and type of privacy and security incidents that occur before and after the training and awareness activities.
9. Conduct spot checks of personnel behavior. For instance, walk through work areas and note if workstations are logged in while unattended or if patient information printouts are not adequately protected.
10. Record user IDs and completion status for web- and network-based training. Send a targeted questionnaire to those who have completed the online training.
11. Have training participants fill out evaluation forms at the end of the class.
12. Identify the percentage of your target groups that participate in training.
13. Determine if you had an adequate number of instructors with the necessary level of expertise for the corresponding training topic.
14. Determine if the training materials addressed all your goals and objectives. Identify the gaps and make a plan to fill them.
15. Review training logs to see trends in attendance.
16. Tape or film participants performing their work after training to determine if they are utilizing the skills taught.
17. Administer occasional tests to personnel. Use multiple choice, short answer, essay tests or a combination. Avoid using true or false tests.
18. Perform interviews with past training participants, as well as personnel who have not yet been trained. Use structured and unstructured interview sessions.

He who dares to teach must never cease to learn. --Richard Henry Dann

Now, brave grasshopper herders, go tackle your awareness and training objectives. Spend time not only on creating awareness and training programs, but also on evaluating the effectiveness of your security and privacy education efforts. You'll find that as you make improvements based upon your evaluations, the grasshoppers you've been herding will metamorphose and you will become not only horse herders, but if you're really good, sheep herders!

Rebecca Herold, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, author and instructor. Rebecca has a B.S. in Math & Computer Science, an M.A. in Computer Science & Education, authored "The Privacy Papers," co-authored "The Practical Guide to HIPAA Privacy and Security Compliance," authored "Managing an Information Security and Privacy Awareness and Training Program," authored "The Privacy Management Toolkit" and several eBooks. She can be reached at rebeccaherold@rebeccaherold.com, http://www.rebeccaherold.com or 515-491-1564.