At the March 2004 Annual Conference of the Federal Information Systems Security Educators’ Association (FISSEA) at the University of Maryland University College campus, Roger P. Quane, PhD, of the National Security Agency in the USA Department of Defense presented a stimulating lecture on “Evaluation Activities: Management’s Nightmare or Dream Come True.”

Dr Quane pointed out that evaluation metrics for training programs, in particular, can be ranked by difficulty as follows:

* Reaction – how participants like the program;
* Learning – what the participants can show they have learned;
* Application – how the participants apply their knowledge in their work;
* Business impact – the effects on how the organization runs its operations;
* ROI (return on investment) – monetary measures of benefit divided by costs required to achieve.

The role of the manager is critical: (s)he leads the project and is responsible for its success. To avoid conflict of interest, the manager should have someone else evaluate the program. Such evaluations are often needed to see if the training program is justified or worthwhile; unfortunately, says Dr Quane, sometimes managers are confronted with a stark choice between honesty and what may seem like professional survival. Regardless of the apparent danger, honesty is the only policy that makes sense. If a program hasn’t worked out, it’s important to say so and take the consequences (“falling on one’s sword” in Dr Quane’s description). In reality, such honest self-appraisal is rarely treated as grounds for dismissal.

In general, Quane recommends that formal evaluations not be applied to projects that cost less than $100,000. In addition, the projects should have organizational visibility, must be needed for organizational success, should be relatively new, and should be requirements driven (i.e., not simply done because everyone has to do it).

Not every training project should be evaluated, says Dr Quane, but it is essential that evaluations be carried out in sequence. First you have to collect information about participation reactions, then you can study how well they learned, and only after that should you look at behavior in the workplace. Each of these levels is more complex and more expensive to measure than the previous one. Measuring effects of training on security is much more complex and will be the subject of a separate article.

* * *

For Further Reading:

Federal Information Systems Security Educators’ Association
<http://csrc.nist.gov/organizations/fissea/>
Membership is free to anyone who wants to join.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.