Psycho-Social Factors in the Implementation of Security Policy.

Part 6. Changing Attitudes Towards Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT 05663-1035 USA

In this series of articles, we are exploring how social psychology helps practitioners implement information security policies more effectively.

Persuasion--changing someone's attitudes--has been described in terms of communications. The four areas of research include

* communicator variables: who is trying to persuade?
* message variables: what is being presented?
* channel variables: by what means is the attempt taking place?
* audience variables: at whom is the persuasion aimed?

Communicator Variables

Attractiveness, credibility and social status have strong effects immediately after the speaker or writer has communicated with the target audience; however, over a period of weeks to a month, the effects decline until the predominant issue is message content. We can use this phenomenon by identifying the senior executives most likely to succeed in setting a positive tone for subsequent security training. We should look for respected, likeable people who understand the issues and sincerely believe in the policies they are advocating.

Message Variables

Fear can work to change attitudes only if judiciously applied. Excessive emphasis on the terrible results of poor security is likely to backfire, with participants in the awareness program rejecting the message altogether. Frightening consequences should be coupled immediately with effective and achievable security measures.

Some studies suggest that presenting a balanced argument helps convince those who initially disagree with a proposal. Presenting objections to a proposal and offering counter-arguments is more effective than one-sided diatribes. The Software Publishers' Association training video, It's Just Not Worth the Risk, uses this technique: it shows several members of a company arguing over copyright infringement and fairly presents the arguments of software thieves before demolishing them.

Modest repetition of a message can help generate a more positive response. Thus security awareness programs which include imaginative posters, mugs, special newsletters, audio and video tapes and lectures are more likely to build and sustain support for security than occasional intense sessions of indoctrination.
Channel Variables

The channel through which we communicate has a strong effect on attitudes and on the importance of superficial attributes of the communicator. In modern organizations, most people assume that a meeting is the ideal way to communicate new information. However, the most effective medium for convincing someone to pay attention to any topic is face-to-face persuasion. Security training should include more than tapes and books; a charismatic teacher or leader can help generate enthusiasm for—or at least reduce resistance to--better security.

In addition, security educators should not introduce new ideas to decision makers in a meeting. There is too much danger of confounding responses to policy with non-policy matters rooted in relationships among the participants. For example, someone might oppose a new policy simply because another executive has supported it. A good way to introduce security policies is to have individual meetings with one executive at a time in which one explains the issues and proposals and asks for support.

Psychologists testing cognitive response theory have studied many subtle aspects of persuasion. For example, experiments have shown that rhetorical questions (e.g., "Are we to accept invasions of our computer systems?") are effective when the arguments are solid but counter-productive when arguments are weak.

Don't use rhetorical questions unless you are absolutely certain that everybody will inevitably have the same answer -- the one you are looking for.

In comparing the central route to persuasion (i.e., consideration of facts and logical arguments) with the peripheral (i.e., influences from logically unrelated factors such as physical attractiveness of a speaker), researchers find that the central route leads to more lasting attitudes and attitude changes.

Audience Variables

As mentioned above, questionnaires and interviews may help cement a favorable change in attitude by leading to commitment. Once employees have publicly avowed support for better security, some will begin to change their perception of themselves. As a teacher of information security, I find that I now feel much more strongly about computer crime and security than I did before I created my courses. We should encourage specific employees to take on public responsibility for information security within their work group. This role should periodically be rotated among the employees to give everyone the experience of public commitment to improved security.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

Copyright © 2000 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.