Psycho-Social Factors in the Implementation of Security Policy.

Part 5. Beliefs and Attitudes

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.

Psychologists distinguish between beliefs and attitudes. "A belief ... refers to cognitive information that need not have an emotional component...." An attitude refers to "an evaluation or emotional response...." Thus a person may believe that copying software without authorization is a felony while nonetheless having the attitude that it doesn’t matter.

Beliefs can change when contradictory information is presented, but some research suggests that it can take up to a week before significant shifts are measurable. Other studies suggest that when people hold contradictory beliefs, providing an opportunity to articulate and evaluate those beliefs may lead to changes that reduce inconsistency.

These findings imply that a new concern for corporate security must be created by exploring the current structure of beliefs among employees and managers. Questionnaires, focus groups, and interviews may not only help the security practitioner, they may actually help move the corporate culture in the right direction.

An attitude, in the classical definition, "is a learned evaluative response, directed at specific objects, which is relatively enduring and influences behavior in a generally motivating way". The advertising industry spends over $50B yearly to influence public attitudes in the hope that these attitudes will lead to changes in spending habits--that is, in behavior.

Research on classical conditioning suggests that attitudes can be learned even because of simple word association. If we wish to move our colleagues towards a more negative view of computer criminals, it is important not to portray computer crime using positive images and words. Movies like "Sneakers" may do harm indirectly by associating pleasant, likeable people with techniques that are used for industrial espionage. When teaching security courses, we should avoid praising the criminals we describe in case studies.

One theory on how attitudes are learned suggests that rewards and punishments are important motivators. Studies show that even apparently minor encouragement can influence attitudes. A supervisor or instructor should praise any comments that are critical of computer crime or which support the established security policies. Employees who dismiss security concerns or flout the regulations should be challenged on their attitudes, not ignored.

When enforcing security policies, too many organizations focus entirely on punishing those who break the rules. However, everything we know about modifying behavior teaches us to use reward rather than punishment. One of my students, a security officer in a large corporation, experimented with reward and punishment in implementing security policies. Employees were supposed to logoff their terminals when leaving the office; however, compliance rates were around 40 percent. In one department, she used the usual techniques: putting up nasty notes on terminals that were not logged
off, reporting violators to their bosses and changing the passwords on delinquent accounts. In a
different department, she simply identified those users who had indeed logged off their terminals
and left a Hershey’s Chocolate Kiss on the keyboard. After one month, compliance rates in the
department subject to punishment had climbed to around 50 percent. Compliance in the
department getting chocolates had reached 80%.

* * *

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.