Psycho-Social Factors in the Implementation of Security Policy.

Part 7. Encouraging Initiative

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.

Wouldn’t it be great if our colleagues actually helped us enforce security policies?

Studies of how and why people help other people have lessons for us as we work to encourage everyone in our organizations to do the right thing. Why do some people intervene to stop crimes? Why do others ignore crimes or watch passively? Two social psychologists, Latane and Darley, have devised a schema that describes the steps leading to prosocial behavior:

* People have to notice the emergency or the crime before they can act. Thus security training has to include information on how to tell that someone may be engaging in computer crime.

* The situation has to be defined as an emergency—something requiring action. Security training that provides facts about the effects of computer crime on society and solid information about the need for security within the organization can help employees recognize security violations as emergencies.

* We must take responsibility for acting. The bystander effect comes into play at this stage. The larger the number of people in a group confronted with an emergency, the slower the average response time. In the words of a standard psychology text, larger groups seem to lead "to a diffusion of responsibility whereby each person felt less personally responsible for dealing with the emergency". Another possible factor is uncertainty about the social climate; people fear appearing foolish or overly emotional in the eyes of those present. We can address this component of the process by providing a corporate culture which rewards responsible behavior such as reporting security violations.

* Having taken responsibility for solving a problem, we must decide on action. Clearly written security policies and procedures will make it more likely that employees act to improve security. In contrast, contradictory policies, poorly-documented procedures, and inconsistent support from management will interfere with the decision to act.

Another analysis proposes that people implicitly analyze costs of helping and of not helping when deciding whether to act prosocially. The combination of factors most conducive to prosociality is low cost for helping and high cost for not helping.

Security procedures should make it easy to act in accordance with security policy; e.g., there should be a hot-line for reporting security violations, anonymity should be respected if desired, and psychological counseling and follow-up should be available if people feel upset about their involvement. Conversely, failing to act responsibly should be a serious matter; personnel policies should document clear and meaningful sanctions for failing to act when a security violation is observed; e.g., inclusion of critical remarks in employment reviews and even dismissal.
One method that does not work to increase prosocial behavior is exhortation. That is, merely lecturing people has little or no effect. On the other hand, the general level of stress and pressure to focus on narrow tasks can significantly reduce the likelihood that people will act on their moral and ethical principles.

Security is likely to flourish in an environment that provides sufficient time and support for employees to work professionally; offices where everyone responds to self-defined emergencies all the time will not likely pay attention to security violations.

Some findings from research confirm common sense. For example, guilt motivates people to act more prosocially. This effect works best when people are forced to assume responsibility. Thus enforcing standards of security using reprimands and sanctions can indeed increase the likelihood that employees will subsequently act more cooperatively.

In addition, mood affects susceptibility to prosocial pressures: bad moods make prosocial behavior less likely, whereas good moods increase prosociality. A working environment in which employees are respected is more conducive to good security than one which devalues and abuses them.

Even cursory acquaintance with other people makes it more likely that we will help them; it thus makes sense for security supervisors to get to know the staff from whom they need support. Encouraging social activities in an office (lunch groups, occasional parties, charitable projects) enhances interpersonal relationships and can improve the climate for effective security training.

***

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.