Psycho-Social Factors in the Implementation of Security Policy.

Part 2. Rationality is Not Enough

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.

Information security policies sometimes seem to evoke strong emotions among our colleagues. People can get very angry about what they perceive as interference with their way of getting their work done. Sometimes people subvert information security by systematically getting around the rules; for instance, on one security evaluation, I noticed a soft-drink delivery man opening the door into a secured area by using the keypad. Startled, I turned to the manager I was interviewing and asked if he had seen this flagrant breach of security; he replied, AOh yeah, no problem. We got tired of opening the door for him every week so we gave him the combination to the lock.@

Psychologists use the word Aschema@ to summarize the complex picture of reality upon which we base our judgements. That manager=s schema included a trustworthy soft-drink delivery man; an information security specialist=s schema in the same circumstances included all the potentially untrustworthy friends of that soft-drink delivery man.

Schemas are self-consistent views of reality. They help us pay attention to what we expect to be important and to ignore irrelevant data. They also help us organize our behavior. For example, our schema for relations at the office includes polite greetings, civil discussions, written communications, and businesslike clothes. The schema excludes obscene shrieks, abusive verbal attacks, spray-painted graffiti and colleagues dressed in swim suits. It is the schema that lets people tell what is inappropriate in a given situation.

Unfortunately, security policies and procedures conflict with most people's schema. Office workers' schema includes sharing office supplies (ALend me your stapler, please?@), trusting their team members to share information (ATake a look at these figures, Sally@), and letting their papers stay openly visible when they have to leave their desk.

Alas, sharing user IDs, showing sensitive information to someone who lacks the appropriate clearance, and leaving work stations logged on without protection are gross breaches of a different schema. Think about access controls: Normal politeness dictates that when a colleague approaches the door we have just opened, we hold the door open for them; when we see a visitor, we smile politely (who knows, it may be a customer). In contrast, access-control policies require that we refuse to let even a well-liked colleague piggy-back their way through an access-card system; security policies insist that unbadged strangers be challenged or reported to security personnel. Common sense tells us that when the Chief Executive Officer of the company wants something, we do it; yet the information security dictates that we should try to train computer room operators to forbid entry to anyone without documented authorization—including the CEO.

If we persist in assuming that we can influence our colleagues to change their perception of information security simply by informing, cajoling, nagging or browbeating them, we will continue to fail.
Information security must be integrated into the corporate culture; such a change needs to use all of the techniques that social psychology can teach us.

**Practical Recommendations**

1. In every security course or awareness program, instructors and facilitators should explicitly address the question of corporate culture, expectations and social schemata. Don’t rely solely on intellectual discourse when addressing a question of complex perceptions and feelings.

2. Address the feelings and perceptions of all participants as they learn about the counter-intuitive behaviors that improved security will demand. Encourage learners to think about how they might feel and respond in various situations that can arise during the transition to a more secure environment. For example, ask participants to imagine

   * asking a colleague not to step through a secured entrance without passing through the access-control system with their own identity;
   
   * telling their boss that they will not copy software without a license to do so;
   
   * walking up to a visitor or employee who is not wearing an identity badge.

3. Use simulations, videos, and role-playing exercises to bridge the gap between intellect and emotion.

   * * *

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.