Psycho-Social Factors in the Implementation of Security Policy.

Part 3. Framing Reality

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.

How can we make the corporate culture more supportive of information security?

In a previous article, I explained that the schema is what social psychologists call the way people make sense of their social interactions. Information security practitioners need to change our colleagues' schema.

Schemas influence what we perceive. For example, an employee refuses to take vacations, works late every night, is never late, and is never sick. A model employee? Perhaps, in one schema. From the security point of view, the employee's behavior is suspect. There have been cases where such people have actually been embezzlers unable to leave their employment: even a day away might result in discovery of their crimes. Saint or sinner? Our expectations determine what we see.

To change the schema so that people take information security seriously, we should provide participants in training and security awareness with real-life examples of computer crime and security breaches so that security policies make sense rather than seeming to be arbitrary.

Schemas influence what we remember. When information inconsistent with our preconceptions is mixed with details that fit our existing schemas, we selectively retain what fits and discard what conflicts. When we have been fed a diet of movies and television shows illustrating the premise that information is most at risk from brilliant hackers, why should we remember the truth—that carelessness and incompetence by authorized users of information systems cause far more harm than evil intentions and outsiders ever do.

Instructors should emphasize the practical side of information security by showing how policies protect all employees against false accusations, prevent damage to the organization=s reputation and profits, and even play a role in national security (especially where business touches the technical infrastructure on which we all depend).

Most important of all, teaching others about information security cannot be an occasional and haphazard affair. Before attempting to implement policies and procedures, we should ensure that we build up a consistent view of information security among our colleagues. In light of the complexity of social cognition, our usual attempts to implement security policies and procedures seem pathetically inept. A couple of hours of lectures followed by a video, a yearly ritual of signing a security policy that seems to have been written by Martians--these are not methods that will improve security. These are merely lip service to the idea of security.

According to research on counter-intuitive information, people's judgement is influenced by the manner in which information is presented. For example, even information contrary to established schemas can be assimilated if people have enough time to integrate the new knowledge into their
world-views. It follows that security policies should be introduced over a long time, not rushed into place.

An effective information security program includes frequent reminders of security. To change the corporate culture, practitioners should use methods such as a security corner in the corporate publication, security bulletins detailing the latest computer crime or security breach that has hit the news, contests for identifying the problems in realistic scenarios, and write-in columns to handle questions about policies. Information security has to become part of the framework of reality, not just an imposition from management.

* * *

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.