Psycho-Social Factors in the Implementation of Security Policy.

Part 8. Dirty Words: Conformity, Compliance and Obedience

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
ADARIO, Inc.

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

These days, many people react negatively to the words conformity, compliance, and obedience. Unfortunately, ignoring social phenomena will not help the security practitioner attain her goals. We have to understand how people work together in reinforcing security policies.

Turning a group into a community provides a framework in which social pressures can operate to improve our organization's information security. People respond to the opinions of others by (sometimes unconsciously) shifting their opinion towards the mode -- the most popular opinion. Security programs must aim to shift the normative values (the sense of what one should do) towards protecting confidentiality, control, integrity, authenticity, availability and utility of data (the Parkerian Hexad enunciated by my respected colleague Donn Parker).

As we have seen in public campaigns aimed at reducing drunk driving, it is possible to shift the mode. Twenty years ago, many people believed that driving while intoxicated was amusing; today a drunk driver is a social pariah. In much the same way, we must move towards making computer crime as distasteful as public drunkenness.

The trend towards conformity increases when people within the group like or admire each other. In addition, the social status of an individual within a group influences that individual's willingness to conform. High-status people (those liked by most people in the group) and low-status people (those disliked by the group) both tend to more autonomous and less compliant than people liked by some and disliked by others. Therefore the security officers should pay special attention to those outliers during instruction programs. Managers should monitor compliance more closely in both ends of the popularity range. Contrariwise, if security practices are currently poor and we want allies in changing the norm, we should work with the outliers to resist the majority=s anti-security bias.

According to social psychologists, AThe norm of reciprocity holds that we should return favors in social relations.@ Even a small, unexpected or unsolicited (and even unwanted) present increases the likelihood that we will respond to requests. For example, members of various religious cults often hand out flowers or books at airports, knowing that the norm of reciprocity will increase the frequency and amounts of donations from basically uninterested passers by.

A security awareness program that includes small gifts such as an attractive mug labeled "SECURITY IS EVERYONE'S BUSINESS" or an inexpensive but useful booklet summarizing security policies can help get people involved in security.

The "foot in the door" technique suggests that we follow a small initial request with a much larger second request. Political field workers, for example, know that they can start small by asking people to let them put candidate stickers in their window; then they ask to put a candidate=s poster on their lawn; eventually they can ask for volunteer time or money. Every compliance with a request increases the likelihood that the person will agree to the next step in the escalating series. It=s as if
agreeing to one step helps to change the target=s sense of themselves. To reduce discomfort about their beliefs and their behavior (what psychologists call cognitive dissonance), they change their beliefs to conform with their behavior.

In our field, we can personally ask an employee to set a good example by blanking their screen and locking their terminal when they leave their desk. Later, once they have begun their process of redefinition of themselves ("I am a person who cares about computer security"), we can ask them for something more intense, such as participating in security training for others (e.g., asking each colleague to blank their screen and lock their terminal). In this way we gradually change the corporate culture so that a majority of people feel personally committed to protecting information assets.

***

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.