CHAPTER 35

Using Social Psychology to Implement Security Policies

M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
Program Chair, Master of Science in Information Assurance
Division of Business and Management
Norwich University, Northfield, VT 05663-1035 USA
mekabay@gmail.com

35.1 INTRODUCTION
35.2 RATIONALITY IS NOT ENOUGH
35.2.1 The Schema
35.2.2 Theories of Personality
35.2.3 Explanations of Behavior
35.2.4 Errors of Attribution
35.2.5 Intercultural Differences
35.2.6 Framing Reality
35.2.7 Practical Recommendations
35.3 GETTING YOUR SECURITY POLICIES ACROSS
35.3.1 Initial Exposure
35.3.2 Counterexamples
35.3.3 Choice of Wording
35.4 BELIEFS AND ATTITUDES
35.4.1 Beliefs
35.4.2 Attitudes
35.4.3 Reward
35.4.4 Changing Attitudes toward Society
35.5 ENCOURAGING INITIATIVE
35.5.1 Prosocial Behavior
35.5.2 Conformity, Compliance, and Obedience
35.6 GROUP BEHAVIOR
35.6.1 Social Arousal
35.6.2 Locus of Control
35.6.3 Group Polarization
35.6.4 Groupthink
35.7 SUMMARY
35.8 **FOR FURTHER READING**

CHAPTER 35

Using Social Psychology to Implement Security Policies

M. E. Kabay

35.1 INTRODUCTION. Most security personnel have commiserated with colleagues about the difficulty of getting people to pay attention to security policies—to comply with what seems like good common sense. They shake their heads in disbelief as they recount tales of employees who hold secured doors open for their workmates—or for total strangers—thereby rendering million-dollar card-access systems useless. In large organizations, upper managers who decline to wear their identification badges discover that soon no one else will either. In trying to implement security policies, practitioners sometimes feel that they are involved in turf wars and personal vendettas rather than rational discourse.

These problems reflect the social nature of human beings; however, they also reflect the fact that although information systems security and network management personnel may have a wide variety of backgrounds, many lack any formal training in social or organizational psychology.

Security policies and procedures affect not only what people do but also how they see themselves, their colleagues, and their world. Despite these psychosocial issues, security personnel pay little or no attention to what is known about social psychology. The established principles of human social behavior have much to teach us in our attempts to improve corporate and institutional information assurance.

Information assurance (IA) specialists concur that security depends on people more than on technology. Another commonplace is that employees are a far greater threat to information assurance than outsiders.

It follows from these observations that improving security necessarily involves changing beliefs, attitudes, and behavior, both of individuals and of groups. Social psychology can help us understand how best to work with human predilections and predispositions to achieve our goals of improving security:

- Research on social cognition looks at how people form impressions about reality. Knowing these principles, we can better teach our colleagues and clients about effective security.

- Work on attitude formation and beliefs helps us present information effectively, and so convince employees and others to cooperate in improving security.

- Scientists studying persuasion and attitude change have learned how best to change people's minds about unpopular views, such as those regarding the security community.

- Studies of factors enhancing prosocial behavior provide insights on how to foster an environment where corporate information is willingly protected.

- Knowledge of the phenomena underlying conformity, compliance, and obedience can help us enhance security by encouraging compliance and by protecting staff against social pressure to breach security.

- Group psychology research provides warnings about group pathology and hints for working better with groups in establishing and maintaining IA in the face of ingrained resistance.

This chapter reviews well-established principles of social psychology that help security and network management personnel implement security policies more effectively. Any recent introductory college textbook in this field will provide references to the research that has led to the principles that are applied to security policy implementation. For this reason, academic references have been kept to a minimum.

35.2 RATIONALITY IS NOT ENOUGH. Information assurance policies sometimes evoke strong emotions. People can get very angry about what they perceive as interference with their way of getting their work done.

Sometimes people subvert IA by systematically getting around the rules. It is not uncommon for regularly scheduled outside delivery and maintenance persons to be given keys, or the door lock combination, for access into secured areas. These people are rarely subjected to security checks, and their potential for intentional or inadvertent damage is great. A common response to new security rules or to attempts at enforcing existing policies and procedures is a charge of paranoia aimed at security personnel. Other accusations include authoritarian behavior and undue interference with job functions. These responses usually indicate a conflict between accepted norms of behavior and the need to change behavior to conform to security principles.

35.2.1 The Schema. Psychologists use the word “schema” to summarize the complex picture of reality upon which we base our judgments.

The schema is what social psychologists call the way people make sense of their social interactions. IA practitioners must change their colleagues’ schemata.

Earlier we mentioned a case in which the manager's schema included supposedly trustworthy delivery people; an IA specialist's schema in the same circumstances includes all the potentially untrustworthy friends of those outsiders.

Schemata 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 know what is appropriate or inappropriate in a given situation.

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

Sharing user IDs, showing sensitive information to someone who lacks the appropriate clearance, and leaving workstations logged on without protection are gross breaches of a different schema—that of the IA specialist. Think about access controls: Normal politeness dictates that when a colleague approaches the door we have just opened, we hold the door open for the person; when we see a visitor, we smile politely—after all, it might be a customer. In contrast, access-control policies require that we refuse to let even well-liked colleagues piggyback 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 (CEO) of the company wants something, we do not oppose it; yet good IA dictates that we 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 IA simply by informing, cajoling, nagging, or browbeating them, we will continue to fail. Information assurance must be integrated into the corporate culture, a process that needs to use all of the techniques that social psychology can teach us.

35.2.2 Theories of Personality. One of the most pervasive obstacles to cooperation in organizations is interpersonal conflict. Many conflicts are rooted in differences of *personality style*. For example, one widely used set of categories for describing people's personalities uses the following schemata:

- Extroversion
    - High: active, assertive, energetic, outgoing, talkative
    - Low: quiet, reserved, shy, silent, withdrawn
- Agreeableness

  - High: affectionate, appreciative, kind, soft-hearted, sympathetic
  - Low: cold, fault-finding, hard-hearted, quarrelsome, unfriendly
- Conscientiousness
  - High: efficient, organized, planful, responsible, thorough
  - Low: careless, disorderly, frivolous, irresponsible, slipshod
- Emotional stability
  - High: calm, contented, stable, unemotional
  - Low: anxious, moody, nervous, tense, worrying
- Openness or Culturedness
  - High: imaginative, insightful, intelligent, original, wide interests
  - Low: commonplace, shallow, simple, narrow interests, unintelligent

The adjectives used in this summary are positive for the "high" side of each trait and negative for the "low" side. However, the assumption that different personality types are easily characterized as superior and inferior seriously interferes with respectful communications among colleagues. For example, people with "low" characteristics might view the preceding summary in this way:

- Extroversion
  - High: nervous, aggressive, excitable, pushy, chattering
  - Low: dignified, respectful, unassuming, attentive, self-sufficient
- Agreeableness
  - High: clinging, gushy, soft-headed, knee-jerk reactive, uncritical
  - Low: stately, analytical, rational, principled, reserved
- Conscientiousness
  - High: obsessive, compulsive, unspontaneous, pompous, slavish
  - Low: free, spontaneous, creative, fun, youthful, having perspective

- Emotional stability
    - High: frozen, ambitionless, boring, dead
    - Low: vibrant, romantic, alive, strong, sensible
- Openness or Culturedness
    - High: flaky, theoretical, complicated, off-the-wall, dilettante
    - Low: earthy, smart, grounded, focused, practical

In discussing corporate culture change, leaders must be on guard to defuse conflicts based on the misperception that one particular response or view of an issue is necessarily good and another necessarily bad. The conflict may be rooted in personality styles rather than in problems of understanding. If the security working group proposes that all employees must challenge anyone in the secured areas who is not wearing a badge, some people—those who have low extroversion, for example—may have a great deal of difficulty with the concept that they should tell anyone else what to do, especially a manager of a higher rank than their own. Arguing over the reasons why such a policy would be useful would sidestep the fundamental problem: that the required behavior is in direct conflict with possibly lifelong and firmly held views on appropriate behavior.

Security personnel must remember that failure to comply with policy is not necessarily the result of a bad attitude.

When it becomes obvious that conflicts are rooted in personality, security personnel will have to try to arrive at a useful compromise. Instead of requiring that everyone confront the unbadged individual personally, the security policies could include a proviso allowing for individuals to choose simply to inform security personnel immediately.

Role-playing exercises sometimes can defuse a problem in accepting security policies by desensitizing resistant personnel. Going through the motions of what they fear or dislike sometimes can help them come to realize that the proposed change in behavior is not as bad as they originally thought. Returning to the example of confronting violations of security, many people have difficulty imagining that they could tell a superior in the management hierarchy not to piggyback. This term, like "hitchhiking" and "tailgating," describes entering through a secured door that has been opened by someone else using a valid access code or token. Going through exercises in which each person pretends in turn to be the upper manager and then the challenger seems to break down resistance to this particular security policy.

In general, leaders of the security team responsible for implementing security policies should be on the lookout for conflicts of style that interfere with the central task of making the enterprise more secure. If an individual likes short, direct instructions without chitchat about nonessentials, the security team member should adapt and stick to essentials; if an individual is

known to like getting to know a stranger and wants to spend 10 minutes learning about family background, it should not be opposed. Communicating ideas in a way that is likely to be acceptable is more important than imposing one's own interpersonal style preferences on others.

Above all, security personnel—and management in general—ought to be doing a great deal more *listening* and a great deal less *commanding*.

35.2.3 Explanations of Behavior. In practice, trying to change corporate culture can be a frustrating and long-drawn-out project. One aspect of this process that security group leaders should monitor closely is the interpretation of employee behavior by members of the security team. In general, people interpret (i.e., explain) other people's behavior according to two independent dimensions: internal or external and stable or unstable. Here are some explanations of why Betty has failed to log off her session for the fourth time this week before leaving the office:

- Internal, stable: "That's just the way she is—she never pays attention to these rules."
- Internal, unstable: "She's been under strain lately because her child is sick—that's why she's forgotten."
- External, stable: "The system doesn't respond properly to the logoff command."
- External, unstable: "This week, the system has not been responding properly to the logoff command."

This simple four-way classification is useful for leaders in understanding and avoiding classic errors of attribution. Such attribution errors can cause conflicts between the security staff and other employees or even among employees with different degrees of compliance to policy.

35.2.4 Errors of Attribution. Some well-established misinterpretations of others' behavior can interfere with the acceptance of security policies. Such errors interfere with the ability of security personnel to communicate the value of security policies. Security group leaders should sensitize their staff to the consequences of these errors.

35.2.4.1 ***Fundamental Attribution Error.*** The most important error people use when explaining other people's behavior is to assume that a person's actions are stable, internal features; a typical example of this error is the naïve belief that an actor's personality is essentially what that person portrays in performance. Anyone who has ever experienced surprise at the demeanor and speech of a favorite actor who is being interviewed has committed the *fundamental attribution error*. Some actors who play bad people have even been verbally and physically assaulted by viewers who cannot resist the fundamental attribution error and genuinely believe that the actors are as bad as the characters they portray.

In security work, being on guard against the fundamental attribution error helps to smooth relations with other employees. For example, if a security group member sees an

employee, Jill, who is not wearing her badge, it is easy to assume that she never wears her badge and is refusing to wear it because of a character flaw. The security officer may act according to these assumptions by being harsh or unfriendly in correcting Jill's behavior. The harshness generates resentment, and Jill may come to associate security with unpleasant people, thus reducing the likelihood that she will comply with policy or encourage others to do so.

In fact, however, most people's behavior is far less stable and internal than unstable and externally based. For example, if the security officer simply asked about the lack of a badge instead of jumping to conclusions, he might discover that Jill's lack of a badge today was due simply to her having taken her jacket off just before an urgent call from the vice president, interrupting her normal procedure of moving the badge from jacket to shirt pocket. Thus, her lack of a badge would not be stable behavior at all—it would be a temporary aberration of no long-lasting significance. Similarly, just by asking, the security officer might learn that Jill normally does wear her badge, but today her four-year-old son took it off her jacket to play with it without his mother's noticing the change. In this example, Jill's behavior is externally based and has nothing to do with character.

By being aware of the fundamental attribution error, security personnel can be trained to adopt a less judgmental, quick-draw mentality that can alienate other employees and damage security programs.

35.2.4.2 ***Actor-Observer Effect.*** The *actor-observer effect* consists of interpreting one's own behavior as appropriate unstable, externally motivated responses to environmental conditions, whereas other people's behavior is viewed in the light of the fundamental attribution error as stable, internally motivated expressions of character traits. Becoming aware of this tendency helps security personnel resist the fundamental attribution error.

35.2.4.3 ***Self-Serving Bias.*** The counterpart of the actor-observer effect is the *self-serving bias*, which fools people into believing that their own behavior is due to stable, internal aspects of their character. Security officers who are unaware of this dangerous error may come to feel that they are in some sense superior to other people who do not know as much about security as they do or who do not comply as fully as they do with security policy. The officers may have failed to integrate the fact that hours of training and coaching by their security group leaders are at least as responsible for their own knowledge of, and compliance with, security policies as any innate superiority.

By bringing this kind of erroneous thinking to light during training and supervision of security staff, managers can help reduce the conflicts that naturally result from an air of assumed superiority.

35.2.4.4 ***Salience and Prejudice.*** When people are asked to guess which person in a group is the most influential (or least influential) person, social psychologists find that whichever person stands out the most, for whatever reason, is more often attributed with the special properties in question. Such effects apply to any characteristic that the psychologists ask about: most (or

least) intelligent, aggressive, sympathetic, and so on. This phenomenon is known as the *salience effect.*

An application of the salience effect might occur if security officers see a group of employees who are violating security policies. A natural and counterproductive tendency is to leap to the conclusion that the tallest or shortest, the thinnest or fattest, the whitest or blackest person in the group must be to blame. This error can result in unfair treatment of perfectly innocent people.

This problem of misinterpreting salience is exacerbated by prejudice; for example, imagine there were an identifiable group called the "Ogunians" who traditionally wear, say, a seven-sided symbol of their identity. If an anti-Ogunian security officer sees a noncompliant group where one of the members is wearing the characteristic heptagon of Ogun, it may be hard for the officer to resist blaming the noncompliance on the Ogunian. Similarly, any minority—whether in terms of gender, gender orientation, religion, race, or disability—can be the focus of a prejudiced security officer's blame when a group disobeys policy. Security leaders should make their staff aware of the danger of applying this erroneous method of explaining group behavior.

Another factor in misinterpreting group behavior is that people can be strongly influenced by expectation—what social psychologists call the *schema*—a subject already introduced. Even observation itself can be biased by expectations; for example, a security officer may believe, erroneously, that (the imaginary group) Ogunians are consistently noncompliant with security policies. Seeing a group of people passing through an open doorway into a secured area without using their badges, the officer may incorrectly report that it was the Ogunian's fault—when, in fact, the Ogunian was waiting to use a valid access card in full compliance with security policy. Such a mistaken report would not only infuriate the innocent Ogunian and possibly cause general Ogunian resentment or hostility toward "security," but it also could mislead the security group itself into trying to correct the behavior of the wrong person or people.

35.2.5 Intercultural Differences. Many countries in the world are experiencing changes in their population due to immigration. Especially in areas where people have heretofore been largely homogenous, cultural, religious, and racial diversity can lead to interpersonal and intergroup conflicts. Such conflicts may be based in part on prejudice, but they also may be the result of differing values and assumptions.

Security personnel engaged in the process of corporate culture change should be sensitive to the possibility that people with different cultural backgrounds can respond differently to proposed security policies. For example, in 2001 the fundamentalist extremists of the Taliban in Afghanistan decreed that non-Muslim people would have to wear badges in public. One can imagine that a Hindu Afghan refugee in the United States who is told to wear a badge for security reasons might believe that its purpose was to mark him as a target -- especially after the terrorist attacks of September 11, 2001. Before pressuring anyone who seems to be resisting a policy, it is valuable to inquire about the person's beliefs and attitudes and to explain the

foundation for the policies in question. Especially where there are intercultural differences, such inquiry and discussion can forestall difficulties and dissension.

35.2.6 Framing Reality. How can we make the corporate culture more supportive of information assurance?

Schemata 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 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 assurance 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.

Schemata influence what we remember. When information inconsistent with our preconceptions is mixed with details that fit our existing schemata, 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 assurance 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. This is especially true where business touches the technical infrastructure on which we all depend.

Most important of all, teaching others about information assurance 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 assurance 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 efforts merely pay lip service to the idea of security.

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

An effective IA 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. IA has to become part of the framework of reality, not just an imposition from management.

35.2.7 Practical Recommendations

- In every security course or awareness program, instructors and facilitators should explicitly address the question of corporate culture, expectations, and social schemata. Do not rely solely on intellectual discourse when addressing a question of complex perceptions and feelings. Use simulations, videos, and role-playing exercises to bridge the gap between intellect and emotion.

- Address the feelings and perceptions of all participants as they learn about the counterintuitive 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 colleagues 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

    - Questioning a visitor or employee who is not wearing an identity badge

35.3 GETTING YOUR SECURITY POLICIES ACROSS. What are some ways to change our colleagues' schemata so that they become more receptive to information assurance policies?

35.3.1 Initial Exposure. Preliminary information may influence people's responses to information presented later. For example, merely exposing experimental subjects to words such as "reckless" or "adventurous" affects their judgment of risk-taking behavior in a later test.

It follows that when preparing to increase employee awareness of security issues, presenting case studies is likely to have a beneficial effect on participants' readiness to examine security requirements.

35.3.2 Counterexamples. Preexisting schemata can be challenged by several counterexamples, each of which challenges a component of the schema. For example, prejudice about an ethnic group is more likely to be changed by contact with several people, each of whom contradicts a different aspect of the prejudiced schema.

It follows that security awareness programs should include many realistic examples of security requirements and breaches. In a counterexample, students in college information assurance courses have commented on the unrealistic scenario in a training video they were shown: a series of disastrous security breaches occurring in the same company. Based on the findings of cognitive social psychologists, the film would be more effective for training if the incidents were dramatized as occurring in different companies.

In practical terms, practitioners should stay current and update their materials. Many IA publications provide useful case studies that will help make awareness and training more effective.

35.3.3 Choice of Wording. Perceptions of risks and benefits are profoundly influenced by the wording in which situations and options are presented. For example, experimental subjects responded far more positively to reports of a drug with "50 percent success" than to the same drug described as having "50 percent failure."

It follows that practitioners should choose their language carefully during security awareness campaigns. Instead of focusing on reducing failure rates (violations of policy), we should emphasize improvements in our success rates. Unfortunately, some rates cannot be expressed in positive terms; for example, it is not easy to measure the success rate of security measures designed to foil attacks on systems.

Judgments are easily distorted by the tendency to rely on personal anecdotes, small samples, easily available information, and faulty interpretation of statistical information. Basically, we humans are not always rational processors of factual information. If security awareness programs rely strictly on presentation of factual information about risks and proposed policies and procedures, they are likely to run up against a stubborn refusal to act logically. Security program implementation must engage more than the rational mind. We must appeal to our colleagues' imagination and emotion as well. We must inspire a commitment to security rather than merely describing it.

35.4 BELIEFS AND ATTIDUDES. 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 correctly that copying a large number of proprietary software packages without authorization is a felony while nonetheless having the attitude that it does not matter to him.

35.4.1 Beliefs. 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 corporate security must explore the current structure of beliefs among employees and managers. Questionnaires, focus groups, and interviews may not only

help the security practitioner, they actually may help move the corporate culture in the right direction.

35.4.2 Attitudes. 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 $50 billion 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 through simple word association. If we wish to move our colleagues toward a more negative view of computer criminals, it is important not to portray computer crime using positive images and words. Movies that show criminal hackers as pleasant, smart, physically attractive, and likable people may do harm by minimizing the seriousness of industrial espionage and cybervandalism. When teaching security, we should avoid praising the criminals we describe in case studies.

Studies of how attitudes are learned consistently show that rewards and punishments are important motivators of behavior. 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 that support the established security policies. Employees who dismiss security concerns or flout the regulations should be challenged on their attitudes, not ignored. Such challenges are best carried out in private to avoid causing embarrassment to the skeptics and possibly generating resistance due to pride or a misplaced sense of machismo.

35.4.3 Reward. 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. A security officer in a large corporation experimented with reward and punishment in implementing security policies. Employees were supposed to log off their terminals when leaving the office, but compliance rates were only around 40 percent. In one department, the security officer 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 percent.

35.4.4 Changing Attitudes toward Security. Persuasion—changing someone's attitudes—has been described in terms of communications. The four areas of research include

1. Communicator variables: Who is trying to persuade?

2. Message variables: What is being presented?

3. Channel variables: By what means is the attempt taking place?

4. Audience variables: At whom is the persuasion aimed?

35.4.4.1 ***Communicator Variables.*** Attractiveness, credibility, and social status have strong effects immediately after the speaker or writer has communicated with the target audience; however, over a period of weeks to a month, the effects decline until the predominant issue is message content. We can use this phenomenon by identifying the senior executives most likely to succeed in setting a positive tone for subsequent security training. We should look for respected, likable people who understand the issues and sincerely believe in the policies they are advocating.

One personality style can be a threat to the success of security policies: the *authoritarian personality*. A body of research suggests that some people, raised by punitive parents highly concerned with social status, become rigidly devoted to conventional beliefs, submit to authority, exercise authority harshly themselves, and are hostile to groups they perceive as unpopular. The worst possible security officer would be an authoritarian person. Such an officer can derive more satisfaction from ordering people around and punishing them than from long-term success in implementing security policies.

35.4.4.2 ***Message Variables.*** Fear can work to change attitudes only if judiciously applied. Excessive emphasis on the terrible results of poor security is likely to backfire, with participants in the awareness program rejecting the message altogether. Frightening consequences should be coupled immediately with effective and achievable security measures.

Some studies suggest that presenting a balanced argument helps convince those who initially disagree with a proposal. Presenting objections to a proposal and offering counterarguments is more effective than one-sided diatribes. The long-used Software Publishers' Association training video, *It's Just Not Worth the Risk*, uses this technique: It shows several members of a company arguing over copyright infringement and fairly presents the arguments of software copiers before rebutting them.

Modest repetition of a message can help generate a more positive response. Thus security awareness programs that include imaginative posters, mugs, special newsletters, audio and videotapes, and lectures are more likely to build and sustain support for security than occasional intense sessions of indoctrination. The use of multiple communications channels (discussed in the next section) also increases the effectiveness of the message.

35.4.4.3 ***Channel Variables.*** The channel through which we communicate has a strong effect on attitudes and on the importance of superficial attributes of the communicator. In modern organizations, most people assume that a meeting is the ideal way to communicate new information. However, the most effective medium for convincing someone to pay attention to any topic is face-to-face persuasion. Security training should include more than tapes and books; a charismatic teacher or leader can help generate enthusiasm for—or at least reduce resistance to—better security.

In addition, security educators should not introduce new ideas to decision makers in a meeting. There is too much danger of confounding responses to policy with nonpolicy matters rooted in relationships among the participants. It is not uncommon for one executive to oppose a new policy simply because another has supported it. A good way to introduce security policies is to have individual meetings with one executive at a time in order to explain the issues and proposals and to ask for support.

Psychologists testing cognitive response theory have studied many subtle aspects of persuasion. Experiments have shown that rhetorical questions, such as "Are we to accept invasions of our computer systems?" are effective when the arguments are solid but counterproductive when arguments are weak. Security officers should not ask rhetorical questions unless they are certain that almost everybody will inevitably have the same answer—the one the security officers are looking for.

Consideration of facts and logical arguments, as the central route to persuasion, has been found to lead to more lasting attitudes and attitude changes than the peripheral influences from logically unrelated factors, such as physical attractiveness of a speaker.

35.4.4.4 ***Audience Variables.*** As mentioned, questionnaires and interviews may help cement a favorable change in attitude by leading to commitment. Once employees have publicly avowed support for better security, some will begin to change their perception of themselves. Specific employees should be encouraged to take on various areas of public responsibility for information assurance within their work group. These roles should periodically be rotated among the employees to give everyone the experience of public commitment to improved security.

To keep up interest in security, regular meetings of enthusiasts to discuss recent security news can keep the subject fresh and interesting. New cases can help security officers explain policies with up-to-date references that will interest their fellow employees and motivate managers to pay attention to security policies.

35.5 ENCOURAGING INITIATIVE. The ideal situation would be for everyone actually to help enforce security policies. Actually, however, some people are cooperative and helpful whereas others—or even the same people in different circumstances—are reluctant and suspicious about new policies. What can be done to increase cooperation and reduce rejection?

35.5.1 Prosocial Behavior. Studies of people who have come to the aid of others can help to encourage everyone in an organization to do the right thing. Some people intervene to stop crimes; others ignore crimes or watch passively. Social psychologists 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.

- Everyone must take responsibility for acting, but the larger the number of people in a group confronted with an emergency, the slower the average response time. Larger groups seem to lead to a *diffusion of responsibility*; each person feels that someone else is more 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. To overcome this effect, a corporate culture must be established that rewards responsible individual behavior, such as reporting security violations.

- Once responsibility for solving a problem has been accepted, appropriate decisions and actions must be taken. 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. There should be a hot line for reporting security violations, and anonymity should be respected if desired. 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. Penalties would include critical remarks in employment reviews and, where appropriate, even dismissal.

One method that does *not* work to increase prosocial behavior is *exhortation*; merely lecturing people about what they ought to do has little or no positive effect.

Significantly, the general level of stress and pressure to focus on difficult tasks with seemingly impossible deadlines can greatly 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 a continuing series of apparent emergencies will not be likely to pay attention to security violations.

Some findings from research confirm common sense. For example, guilt motivates many 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 subsequently will act more cooperatively; however, as suggested earlier, punishment should not replace reward.

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 that 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 (e.g., lunchtime discussion groups, occasional parties, and charitable projects) enhances interpersonal relationships and can improve the climate for effective security training.

35.5.2 Conformity, Compliance, and Obedience. These days, many people react negatively to the words "conformity," "compliance," and "obedience," but ignoring social phenomena will not help security practitioners to attain their goals. Despite the unpopularity of this subject area, it is valuable to understand how people can work together in reinforcing security policies. The following sections look at how to increase conformity, compliance with security rules, and obedience to IA authorities.

35.5.2.1 ***Social Pressure and Behavior Change.*** Turning a group into a community provides a framework in which social pressures can operate to improve an organization's information assurance. People respond to the opinions of others by shifting their own opinions, sometimes unconsciously, toward the mode—the most popular opinion. Security programs must aim to shift the normative values, the sense of what one should do, toward protecting confidentiality, possession or control, integrity, authenticity, availability, and utility of data.

35.5.2.2 ***Changing Expectations.*** As has been evident in public campaigns aimed at eliminating drunken driving, it is possible to shift the mode. Thirty years ago, many people believed that driving while intoxicated was amusing; today, a drunken driver is a social pariah. High school children used to kill themselves in large numbers on the nights of their high school proms; today, many children spontaneously are arranging for safe rides home. In much the same way, we must move toward making computer crime as distasteful as public drunkenness.

The trend towards similar behavior 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 to group standards. 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, security officers should pay special attention to those outliers during instruction programs. Managers should monitor compliance more closely at both ends of the popularity range. If security practices are currently poor, and allies are needed to change the norm, working with the outliers to resist the majority's anti-security bias may be the most effective approach.

35.5.2.3 ***Norm of Reciprocity.*** According to social psychologists, the norm of reciprocity indicates that, in social relations, favors are usually returned. Even a small, unexpected, unsolicited, or even unwanted gift 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 amount of donations from basically uninterested passersby.

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.

35.5.2.4 ***Incremental Change.*** The foot-in-the-door technique suggests that a small initial request should be followed by an even larger second one. 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 an escalating series. It is as if agreeing to one step helps to change the targets' sense of themselves. To reduce discomfort about their beliefs and their behavior (what psychologists call "cognitive dissonance"), people change their beliefs to conform with their behavior.

Employees can be asked personally to set a good example by blanking screens and locking terminals when leaving their desks. Later, once they have begun the process of redefining themselves ("I am a person who cares about computer security"), they can be asked for something more intense, such as participating in security training by asking others to blank their screens and lock their terminals. The same methods could be used to accomplish similar ends, and in this way the corporate culture would be changed so that a majority of people feel personally committed to good security practices.

35.6 GROUP BEHAVIOR. Some groups of people are referred to as teams, while others are called gangs. Social psychological insights into group behavior can improve success rates for IA policies.

35.6.1 Social Arousal. Studies on the behavioral effects of being in groups produced contradictory results; sometimes people did better at their tasks when there were other people around, and sometimes they did worse. Eventually, psychologists realized that the presence of other people is socially arousing; that is, people become more aware both of their own behavior and of social norms when they are in groups. Social arousal facilitates well-learned habits but it inhibits poorly learned habits. Thus, when trying to teach employees new habits to improve security, it is counterproductive to put them into large groups. Individualized learning (e.g., by means of computer-based training and videotapes) can overcome inhibitory effects of groups in the early stages of behavioral change.

35.6.2 Locus of Control. Another factor that interferes with implementation of security policies is the *locus of control.* People do not like feeling that they have no control over their

environment. For example, in a classic experiment reported in social psychology textbooks, two equivalent teams of people were both subjected to loud and disruptive noise coming through a loudspeaker in their work area. One group had no control whatever over the noise, whereas the other had a large button with which they could stop the noise at once. The group with the stop button did noticeably better at their complex task than the other group—yet in no case did anyone actually press the button. Simply feeling that they *could* exert control if they wanted to significantly altered the performance of the experimental subjects.

Similarly, in studies of healing among older patients, three groups were defined: (1) controls, (2) people given a plant in a pot, and (3) people given a plant in a pot plus instructions to water it regularly. The third group did significantly better than the second in their recovery. Once again, the sense of control over the environment appeared to influence outcomes.

In security policy implementation, experience confirms that those organizations with the most participation and involvement by all sectors do best at developing and implementing information protection plans. A common phrase that refers to this phenomenon is "buy-in," as in "The different departmental representatives felt that they could genuinely buy into the new policies because they had fully participated in framing them."

35.6.3 Group Polarization. Another branch of research in group psychology deals with group polarization. Groups tend to take more extreme decisions than would individuals in the group acting alone. In group discussions of the need for security, polarization can involve deciding to take more risks—by reducing or ignoring security concerns—than any individual would have judged reasonable. Again, one-on-one discussions of the need for security will generally be more effective in building a consensus that supports cost-effective security provisions than will large meetings.

35.6.4 Groupthink. In the extreme, a group can display groupthink, in which a consensus is reached because of strong desires for social cohesion. When groupthink prevails, evidence contrary to the received view is discounted; opposition is viewed as disloyal; dissenters are discredited. Especially worrisome for security professionals, those people in the grip of groupthink tend to ignore risks and contingencies. To prevent such aberrations, the leader must remain impartial and encourage open debate. Respected security consultants from the outside could be invited to address the group, bringing their own experiences to bear on the group's requirements. After a consensus—not the imposition of a dominant person's opinions—has been achieved, the group should meet again and focus on playing devil's advocate to try to come up with additional challenges and alternatives.

In summary, security experts should pay attention to group dynamics and be prepared to counter possible dysfunctional responses that interfere with acceptance of information assurance policies.

35.7 SUMMARY. This chapter has reviewed the major findings of social psychology that can help to improve information assurance programs. These ideas can prove useful to readers who think about social psychology as they work to implement security policies.

- Recognize that information assurance policies often conflict with the schema for trusting, polite behavior in situations outside the work arena.
- Train information assurance personnel to recognize that failure to comply with security policies may be rooted in many other factors than simply bad attitude.
- Listen more than you command.
- Teach security personnel to avoid the classic errors of attribution when trying to understand their colleagues' motivations.
- Openly discuss and counter prejudice before it causes conflicts.
- Take intercultural differences into account when setting and implementing security policies.
- Before attempting to implement policies and procedures, ensure a consistent view of information assurance among colleagues.
- Security policies should be introduced over a long time, not rushed into place.
- Presenting case studies is likely to have a beneficial effect on participants' readiness to examine security requirements.
- Security awareness programs should include many realistic examples of security requirements and breaches.
- Attempt to inspire a commitment to security rather than merely describing it.
- Emphasize improvements rather than reduction of failure.
- Create a new concern for corporate security by exploring the current structure of beliefs among employees and managers.
- Never portray computer crime using positive images and words.
- Praise any comments that are critical of computer crime or that support the established security policies.
- Employees who dismiss security concerns or flout the regulations should be challenged on their attitudes, not ignored.
- Identify the senior executives most likely to succeed in setting a positive tone for subsequent security training and engage their cooperation to act as role models.

- Frightening consequences should be coupled immediately with effective and achievable security measures.
- Presenting objections to a proposal and offering counterarguments is more effective than one-sided diatribes.
- Security awareness programs should include many, frequent, and preferable novel and entertaining reminders of security issues.
- In addition to tapes and books, rely on a charismatic teacher or leader to help generate enthusiasm for better security.
- Encourage specific employees to take on public responsibility for information assurance within their work groups.
- Rotate security roles periodically.
- Security training should include information on how to tell that someone may be engaging in computer crime.
- Build a corporate culture that rewards responsible behavior, such as reporting security violations.
- Develop clearly written security policies and procedures.
- Security procedures should make it easy to act in accordance with security policy.
- Treat failures to act in accordance with security policies and procedures as very serious matters.
- Enforcing standards of security can increase the likelihood that employees will subsequently act more cooperatively.
- A working environment in which employees are respected is more conducive to good security than one that devalues and abuses them.
- Get to know the staff from whom you need support.
- Encourage social activities in the office.
- Pay special attention to social outliers during instruction programs.
- Monitor compliance more closely at both ends of the popularity range.
- Work with the outliers to resist the herd's antisecurity bias.

- Include small gifts in your security awareness program.
- Start improving security a little at a time, and work up to more intrusive procedures.
- Before discussing security at a meeting, have one-on-one discussions with the participants.
- Remain impartial and encourage open debate in security meetings.
- Bring in experts from the outside when faced with groupthink.
- Meet again after a consensus has been built and play devil's advocate.

35.7 FOR FURTHER READING

Lippa, R. A. *Introduction to Social Psychology,* 2nd ed. Belmont, CA: Brooks/Cole Publishing Div. of Wadsworth, 1994.

Myers, D. G. *Social Psychology,* 4th ed. New York: McGraw-Hill, 1991–1993).

