Corporate computer crime and abuse policy statement

by RICHARD CASHION
Tennessee Technological University
Cookeville, Tennessee

SURVEY

In the Spring of 1986 the Data Processing Management Association (DPMA) conducted a survey of its members and a random selection of corporate CEO’s to determine the general attitude toward a Corporate Computer Crime and Abuse Policy Statement. DPMA conducted this survey as a starting point in developing a model policy statement. 181 surveys were returned. Of those responding only 27 percent of the organizations have a published policy statement; 10 percent were working on one. At the same time, only 5 percent of the responses indicated that a policy statement was not needed.

WHY HAVE A POLICY STATEMENT?

DPMA feels that it is important for each organization to have a published Computer Crime and Abuse Policy Statement. Without a published statement, certain computer crimes will go unpunished even when the culprit is caught. Most computer crime legislation uses the term “unauthorized” in every area to describe the criminal act. The organization must take steps to ensure that everyone in the organization is aware of his/her authorization and responsibilities in respect to computerized information and the computer itself. If it does not, the only legal remedy that the organization may have is to fire the individual involved.

WHO SHOULD DEVELOP THE POLICY STATEMENT?

It is clear that the policy statement should be endorsed by top management. However, it may not be as clear that top management must be involved in its development with guidance from the MIS, legal, and security staff. Top management must realize the full impact of the change in our resource base. America is moving from an industrially-based to an information-based society. Information has become a valuable resource in the same way that people, building, equipment, and money are considered valuable resources. It is becoming increasingly clear that the success of any institution is more and more dependent on its ability to create, store, retrieve, transfer, and protect vast amounts of information.

WHAT SHOULD BE IN THE POLICY STATEMENT?

The goal of the policy is to make a short concise statement about the organization’s views of computer crime and abuse. The statement should not spell out the detail procedures. There should be several levels of detail in the overall policies and procedures for computer crime and abuse. Some large organizations start with a “policy statement” of one or two pages. Then the policy statement is broken down into “standards.” The standards expand on the policy and provide more detail for the development of the “minimum requirements statement.” The minimum requirements statement defines the minimum general procedures that must be followed to conform to the policy. The next level is the actual “procedure manuals.” This many levels are needed in a very large multi-division organization. In most organizations only two levels are needed.

The one or two page policy statement is the focal point of the entire operation and must lay a foundation for the procedures.