Corporate Exposure: Organizational Theft (Part I)

Harry P. Mirijanian

Recent articles have reported that American businesses are losing anywhere from $40 billion to $100 billion each year to theft of materials, products, or money by employees. Even the conservative figure is staggering—but why is there such a large variance? The answer is simple if unnerving: Many companies have not yet uncovered their losses, which are unwittingly absorbed into general operating overhead expenses. Worse yet, some companies that are aware of their losses choose not to report them because they fear the negative publicity that would surround such an admission.

Perhaps the more important question is where the losses are coming from. The plain truth is that *every type of organization is susceptible to loss from employees at all levels.*

Deficient protection

Unfortunately, over the past 20 years we have seen numerous examples of deficiencies in organizations that give rise to these types of losses. What we plan to do in the next three columns is outline some of the controls companies can put in place to reduce this exposure, discuss details regarding some of the losses we have noted, and highlight the insurance coverages available to help transfer a portion of the risk.

As long-time readers of this column know, we always advise our clients to operate their business under the presumption that they have no insurance. I often ask them what they would do differently if in fact they really did have no coverage. Let us begin our discussion here devoid of any insurance implications.

Establishing controls

Establishing organizational controls is the first vital step in addressing this particular exposure. If employees believe that their criminal activity could be uncovered, naturally they will be less inclined to steal. The absence of any sort of internal controls, or failure to enforce any existing procedures, leaves the company completely unprotected and at the mercy of unscrupulous workers. You should begin with what I consider the simplest and easiest controls to implement: those that include physical barriers. Safes and vaults are a good means of protecting cash and vital records. We have encountered companies that have such units but then make mistakes. For example, often the combinations are known by far more people than is necessary; the result is easy access for potential thieves. Or the combinations are never changed—another mistake. Combinations should be changed at least every few months—and immediately after someone who has the combination has been terminated.

Padlocks are other useful tools that tend to be misused. Many companies have security gates and window bars that are secured by padlocks. But they leave the locks open during the day, just hanging on their hooks. Criminals have been known to switch a padlock with a similar one of their own. Thus, when you secure the lock at night, you are securing the thief's lock. The thief returns later that night, opens the lock, steals your inventory, and replaces *your* lock upon leaving. When you return the next morning, there is no sign of any trouble. This sort of theft can go undetected for a long time.

Door locks can be compromised quiet easily, especially since it is often easy for employees to accumulate keys to everything from the executive washroom to the cashier's office. Controlling distribution of keys is one step, as is periodically changing the locks.

Many organizations rely on security alarms to protect their inventory. We have seen two significant problems with this type of protection. First, the installations are often faulty. I believe that there are only two states that require alarm installers to be bonded and certified. We have heard of cases in which criminals were able to bypass a security alarm because they knew the system's Achilles heel.

The second problem is that often the wrong equipment is installed. We recall one warehouse in which motion detectors were installed. Unfortunately, the inventory was stacked high enough that it blocked the motion detectors' ability to "see" movement below a certain level. We have also seen residential alarms used in commercial properties. Clearly, lacking the right equipment and installation means a system that will provide extremely poor protection. (Remember, if your state requires some sort of certification, be sure to check that your installer has the proper credentials.) ■

Harry P. Mirijanian is president of Applied Risk, an independent risk services management firm established to assist the business community in reducing exposure to loss and insurance costs. He is a frequent speaker at AMA seminars.

Published as a supplement to the July-August 1997 issue of *Management Review.*

Finance Forum Editor: George Milite.
Forum Group Editor: Florence Stone.
Senior Editorial Assistant: Grace Lander LoPinto.
Graphic Artist: Tony Serio

 Editorial offices: 1601 Broadway, New York, NY 10019; tel: 212-903-8073; fax: 212-903-8083; e-mail: fstone@amanet.org.

For a single copy request, telephone UMI InfoStore at 1-800-248-0360 (overseas, 415-433-5500).

Additional *Forum* subscriptions are available to members at $40 each. Contact Membership Department, AMA, 1601 Broadway, New York, NY 10019. For sample issues, call the Editorial Office at (212) 903-8073.