

# Combatting Workplace Fraud:

## *Successfully Integrating the Security and Internal Audit Functions*

Robert Schuller

Imagine this scenario: An employer has a peak staffing load of 2,500 people. Well over 90% of this staff is between 15 and 17 years old and for most staff members, this is their first job. They are paid only a quarter or two an hour more than minimum wage, yet over the course of every eight-hour shift, most will ring up over one thousand dollars in cash revenue. Their immediate supervisor is another teenager, perhaps with just a month's more experience.

This setting—a nightmare for internal auditors and business owners alike—is the daily reality for most of the regional theme park industry. The potential problem, however, is not limited to theme parks. For many of the nation's top entertainment and retail companies, young, seasonally-employed labor makes up a significant portion of their workforce. The risks inherent in their environment and operations require a response greater than that provided by a traditional internal auditing program alone. The challenges faced by theme parks and many other companies with similar employee-based risks—such as restaurants, clothing stores, and movie theaters—require a sophisticated integration of the internal audit and the traditional security functions. For this article we, as do many others, call this combined function *loss prevention*.

### **The Integrated Response**

Both the security and the internal audit functions are concerned with asset protection, including physical and tangible assets such as cash, plant, property, equipment, and the like. These functions also protect the intangible assets of a company, such as information, time, and the company's reputation. Unfortunately, traditional security practitioners usually lack basic auditing skills and the knowledge of internal control design, implementation, and evaluation. On the other hand, internal auditors aren't usually trained in investigation management skills such as suspect interviewing, physical and electronic surveillance, criminal law, legal case preparation, and restitution management.

Because of the differences between the two disciplines, combining the internal auditing function and the traditional security function can create powerful synergies. Security excels in response and resolution, while internal auditing excels in detection, follow-up, and correction. The ability of a combined team or department to detect, respond to, correct, dispose of, and prevent operational deficiencies can be incredible. In order to achieve this level of sophistication, a comprehensive infrastructure must be in place to allow for functional integration and control of the combined

departments. The integrated response to these threats can be classified according to the type of control each represents.

### **Prevention**

As with all internal auditing endeavors, top management support is essential. The loss prevention effort, whether or not operated separately from the internal auditing department, must have the full backing of the Board of Directors. This in turn encourages strong backing from the CEO, and having the CEO as a loss prevention champion is tremendously helpful. Emphasizing the positive effects of a properly run loss prevention department on the bottom line—or lack thereof—may be helpful in gaining interest from reluctant top management.

The next most important infrastructure element is a properly designed Human Resources area. First, thorough policies and procedures should be put in writing, distributed to all employees, and covered during new hire training. Of special importance are well written cash handling procedures, which clearly define and prohibit the methods or behaviors connected with theft and misappropriation.

Second, the loss prevention atmosphere should be extended to the hiring proc-

ess. Inform applicants that the company conducts criminal history and sex offender checks on every applicant and employee, regardless of position. This alone will sometimes reduce the number of “bad apples” who attempt to apply. Applicants who admit to prior criminal histories are generally excluded from security-sensitive positions. Applicants who falsify employment applications by concealing convictions are not hired. If an existing employee fails to properly disclose criminal convictions, he or she is terminated. Most companies have a multi-tiered interview process, with increasingly thorough interviews conducted first by the human resources department and then by an applicant’s department representative. The interviewer in each step of the process should make some positive statement about the company’s loss prevention policy. Also, loss prevention personnel should conduct a security interview with applicants for all security-sensitive and all upper management positions.

Third, emphasize the importance of loss prevention during training. Most large companies, like theme parks, will have a general orientation session conducted by the human resources department, followed by more specific departmental training, and, as the job requires, cash handling training. Loss prevention topics, especially concerning the direct consequences to the employee if he or she is involved in a loss or misappropriation, should be discussed at all levels of training, beginning in orientation. In larger companies, it may be possible to have loss prevention personnel act as ‘guest speakers’ during the orientation session. Cash handling training should be conducted separately from departmental training to emphasize its importance. A company’s revenue control or finance department might best conduct this training. If these departmental resources aren’t available, the ad hoc cash handling trainer should have sufficient experience with and familiarity with cash handling procedures and the importance of the internal controls associated with those policies.

All of these human resource elements put employees, especially new hires, on notice that their employer takes loss seriously and will act swiftly to prevent and detect losses. By cultivating an attitude of loss-intolerance in employees, a company will have made great strides in reducing potential loss by making it more difficult for employees to rationalize theft. However, a company’s infrastructure alone will not dissuade every employee from committing fraud. Once a company has crafted the right environment with its employees, it must develop strong detection capabilities.

### **Detection**

This is the area of greatest synergy between security and internal auditing. Detection controls can be classified as either passive or active. The first detection control that a company should put in place is a telephone reporting system through which employees can report theft incidents, anonymously if they choose. The reporting system should also encourage the reporting of other loss-related issues, such as safety and sexual harassment concerns, although other departments within the company may ultimately investigate incidents of this type.

The strengths of the internal auditor can lend tremendous assistance to a second passive detection control—the data-mining project. Whether using customized software or just “elbow grease,” the loss prevention department should purposely mine the company’s financial and operational databases for information indicating potential losses. This research usually has little evidentiary value, but it is unequalled as a means of pointing additional loss prevention resources toward the amelioration of further loss.

The active detection controls are the primary tools of the loss prevention department. Starting at the top of the department, every loss prevention employee should be required to observe and report on various conditions within the company. Loss prevention supervisors will conduct “area audits” on a specific location, shop, revenue stand,

etc. The area audit is a checklist, much like an internal control questionnaire, on which the auditor indicates the absence or presence of a pre-established condition and any relevant comments. Audited locations are selected both at random and in response to direction from either prior investigations or results from data mining. The auditor will conduct the audit without the assistance of the audited department’s personnel and, immediately upon its completion, will contact the area’s immediate supervisor if he or she was not present. By reviewing the area audit results immediately with the audited-supervisor present to see and correct any deficient conditions, corrective action can be taken or praise for a positive audit can be given on the spot. Area audits do not replace the formal internal audit report, which can take several weeks or longer for the internal auditing department to prepare and for the audited department to respond. Instead, area audits are a way of immediately addressing operational issues that have high loss risk. Results of area audits, especially progressive improvement, should be summarized and included in the formal audit reports.

Physical surveillance is another valuable loss prevention tool, and it too comes in two varieties: plainclothes and undercover. Plainclothes investigators are hired by the loss prevention department and trained therein. They roam about the company property dressed like other customers, looking for specific violations of company policy or outright theft. The main differences between plainclothes investigators and the typical ‘secret shopper’ are what level of specialized company-specific training the investigator has received and what is included in the scope of the investigator’s survey. Secret shoppers focus only on “softer” issues like the quality of customer interaction, employee friendliness, and store cleanliness. A loss prevention department may wish to use secret shoppers to supplement its core of plainclothes investigators with unknown faces.

In contrast, undercover investigators are hired by a department (usually un-

knowingly) and trained as an employee in that area. They are assigned to a real work location and are able to observe from an insider's perspective. However, they also receive additional loss prevention training on basic investigative techniques and on how to covertly report their findings. It goes without saying that only the loss prevention manager should know the identities of the undercover investigators.

Most theme parks and some larger retail establishments will also have a uniformed security force. Although only a very bold employee would steal in sight of a security officer, the security force can be another valuable asset to the loss prevention department, beyond mere deterrence. Besides having primary responsibility for protecting the company's assets outside business hours, the security force can alert the loss prevention department to developing trends in security areas unrelated to theft.

## Correction

After the detection controls have identified a loss, the correction controls must see that the responsible parties are identified, weak or defective controls are replaced, and the company recovers its losses. The loss interview is the single most powerful tool toward this end. Investigators, trained in specialized interviewing techniques, use a low-pressure method to obtain a confession for prosecution (when appropriate) and elicit from the suspect an understanding of where the control system failed. If the investigator fails to obtain data about the cause of the loss, he or she has failed as an internal auditor. Likewise, failing to secure the information needed to properly terminate and/or arrest a theft perpetrator is an equal disservice to the employer. This is the true integration of internal auditing and loss prevention.

Loss prevention personnel, preferably with high standing within the com-

pany's general management hierarchy, should attend significant management meetings and report recent findings, make progress reports on pending cases, and praise managers for their efforts in successfully reducing loss. Formal internal audit reports, including the results of investigations and the loss prevention department's suggested corrections to controls and policy, should be distributed to the appropriate management personnel and require a written response and follow-up plans. A summary of this information should be provided to the larger workforce by way of loss prevention bulletins.

## Conclusion

There are many inherent fraud risks for a seasonal employer. Successfully overcoming these threats requires a combination of traditional security functions and internal audit functions. The resulting best practices transform imposing business threats into manageable business challenges.

*Robert Schuller is the founder of Schuller & Associates, a management consulting firm targeting the problems of growing businesses, including internal control and loss prevention issues. He was a loss prevention supervisor in the theme park industry from 1991 to 1997.*