Are these isolated incidents? Not according to the Association of Certified Fraud Examiners (ACFE). In its "2010 Global Fraud Study," the ACFE investigated fraud cases in the United States and in over 100 other countries and reported that organizations lose 5 percent of their annual revenues (or, approximately $2.9 trillion) to fraud.

The ACFE study notes that fraud can happen at any level of a company, from the mailroom employee to the account executive to the senior executive. While fraud is more prevalent at lower levels, the damage is usually more substantial when high-level executives are involved. The ACFE found that the median loss when owners/executives are involved ($723,000) was more than six times the median loss caused by managers ($200,000) and more than nine times that involving lower-level employees ($80,000).

Despite the examples cited above, losses are not limited to major corporations. Small businesses are often the hardest hit by employee fraud. Almost half of the fraud cases studied by the ACFE involved small businesses, with the median loss pegged at almost $100,000, a difficult amount for any company to lose, let alone a small business with limited resources.

An effective control is to have a separation of duties whenever employees handle money. For instance, if one employee reviews invoices and authorizes payment, then a second employee should write and send the check, and yet another employee should reconcile the bank statements.

In addition to a separation of duties, redundancy is also a powerful control. This means having more than one person look at the same transaction. For example, checks should be cosigned rather than authorized by only one person, and multiple employees should have responsibility for overseeing specific bank accounts preventing one employee from "lapping" or moving funds from account to account ahead of any audit so that no irregularities are detected.

Centralized processes also allow tighter control. When procurement is centralized, employees in satellite offices are not able to buy more than needed and then resell or return items for cash. When inventory is centralized, employees know that the company's assets are tracked and monitored.

Internal controls should also be used to detect fictitious vendors. In addition, processes should be in place to verify that vendors exist, that they are performing their duties for the company, and that payment is in line with the services provided.

While internal controls are vital, they are not the only way to detect and to discourage employee fraud. In fact, today more fraud is found by accident than through the strength of internal controls. However, neither tops the list of how fraud is detected. The ACFE found that almost 40 percent of fraud is discovered through tips, the majority of which come from employees. Customers, vendors, and anonymous callers are also good sources.

Another mechanism for controlling employee fraud is to institute careful hiring practices, although this approach is less effective than strong internal controls or a forum for tips. Unicru, a company that specializes in helping other companies recruit and hire employees, has found that 70 percent of "internal shrinkage," or theft by employees, is carried out by people who are on the job for less than 30 days. Eliminating job candidates who have a track record of holding prior jobs for fewer than 90 days is one way to limit exposure to shrinkage.

Checking job applicants for criminal backgrounds makes good business sense. However the ACFE found that only 15 percent of the fraud-committing employees had a previous conviction. In addition, employment-screening processes may vary from country to country, which can be challenging for large, multinational firms. Weeding out bad apples is important, but not nearly as important as setting up internal systems to discourage fraud before it begins.