Managing

BY STEPHEN PEDNEAULT

Protecting Company Coffers

The right internal controls can help a company prevent or detect insider fraud schemes before serious losses occur.

MILD-MANNERED, soft-spoken, 50-year-old David and his wife of 20 years still lived in the first house they ever owned. David maintained a daily routine that included rising early every morning, working out at the gym, and arriving early at work. Dedicated to his staff and his responsibilities as controller for World Manufacturing (WM), he ended his workday by five each evening, and retired to bed early each night. He cared for his elderly parents, who lived out of state, visiting them almost monthly to attend to their health and other needs. He was also stealing from the company. By the time he was caught, he had embezzled $1.8 million.

Though the names of all parties have been changed, the above scenario was based on a true story. Of course, embezzlers don't always fit a profile, and companies should establish basic procedures that apply to all employees who have access to company funds. But this case, as explained in this analysis, is one example that can serve as a cautionary tale to any company.

WM relied on foreign suppliers and manufacturing in China and other parts of the world. The company's 50 employees sourced their product sales outside of the country, with final assembly and packaging performed locally for domestic sales. Annual domestic sales exceeded $10 million.

Bill, general manager, and Harold, one of the owners, oversaw production, sales, operations, and finance.

On January 1, 2010, WM was closed for the holiday. While at home, Harold received a call from Bill, who had just read an article in the local paper. The article reported that police had arrested David for soliciting a prostitute. According to the article, David had been the target of a police stakeout at a condominium complex. The residents of the complex noted that David frequented the unit at different times during the day, accompanied by different women. From the address of the condominium unit in question, Harold quickly realized David had purchased the unit some time ago on behalf of WM to provide housing for visiting owners, employees, suppliers, and others for business purposes. Harold immediately placed David on paid administrative leave, changed the locks and access codes, and began an investigation into David's background as well as his financial activity at WM.

Harold met with individuals in the finance department and informed them of David's absence. Harold then solicited their assistance in obtaining past bank statements and other accounting records. Throughout the day, they located boxes of records in various departments and brought them to a staging area in the conference room. The team then proceeded to analyze the files, particularly those containing WM's financial information.

WM maintained one primary checking account used for operations, as well as several other accounts at various institutions. Staff located the statements for these accounts covering the most recent months' activity. Harold also went online and generated statements for these accounts for the same time period.

As Harold reviewed the bank statements, he realized **continued on page 106**

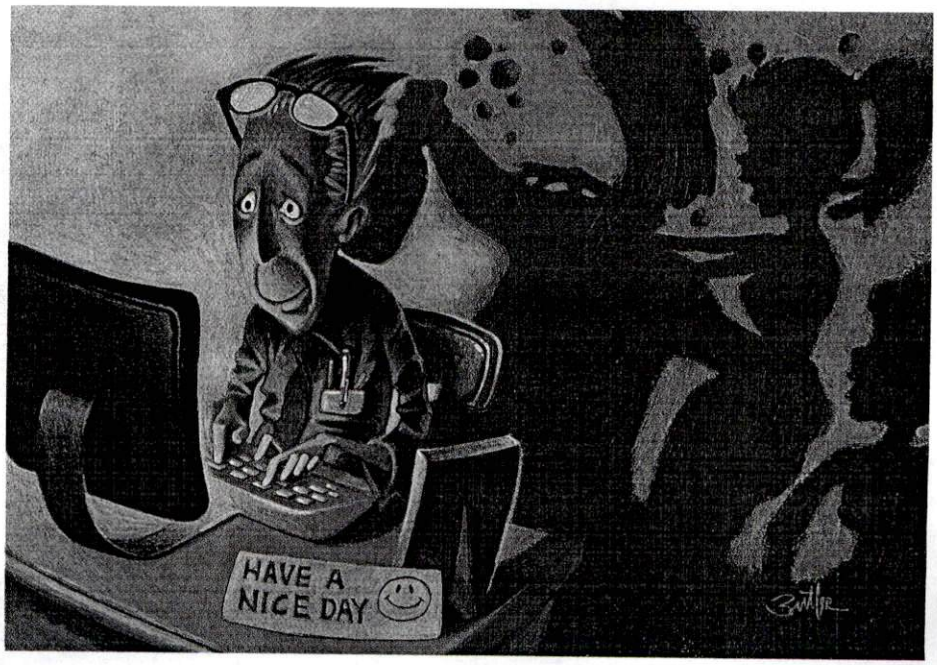

ILLUSTRATION BY RALPH BUTLER

continued from page 108

that David had obtained a debit card drawn on a WM account. Harold also saw that various female names appeared on electronic transfers made each month. Harold added up the identified transactions during the six-month period and estimated that the company suffered a loss of $50,000.

The search for bank statements and records beyond the prior six months proved unfruitful. The WM team could not find any of the statements, canceled checks, or other associated records. Harold began communicating with the banks, ordering monthly bank statements and canceled check images for each bank account for the past five years. He segregated the records by month and year, and started his detailed review of each month's activity. He also created an Excel spreadsheet, keeping track of unauthorized transactions appearing on the bank statements.

Highlighted bank statement pages and canceled check images supported his Excel spreadsheet. Harold focused his attention on the bank records until he finished analyzing information from the previous five years. When he had completed his review, the preliminary results floored him, as his spreadsheet now included more than $1.6 million in unauthorized purchases, checks, wire transfers, withdrawals, and debit card transactions. David had been with the company for six years and had been stealing for four of those years.

Once the scope of the fraud became apparent, the company hired an attorney, a forensic accountant, and a computer forensic specialist. Harold also called the police to prevent David from fleeing the country.

In searching other areas of financial responsibilities under David's control, Harold identified where David had processed additional unauthorized payroll to himself and several other employees of WM. David also oversaw and managed WM's retirement plans and contributions. He had pilfered from that area as well, contributing additional unauthorized company funds to his retirement account as well as the accounts of other employees, including the account of Bill, Harold's general manager. The final fraud total was $1.8 million.

Confronted with these findings and supporting evidence, David confessed to his crimes. He indicated that Bill never participated in any of the fraudulent activity. David said that he worked alone in the thefts. No evidence was ever obtained that implicated Bill.

> "Companies should consider conducting background updates if red flags appear in an employee's behavior."

David claimed he fell victim to a midlife crisis. He detailed a secret second life that began more than four years earlier. It included near-monthly trips overseas to visit women in China. He covered these excursions with the ruse of traveling to Florida to care for his parents.

He identified several other schemes, including obtaining and using a bank debit card for personal purposes, altering signed checks for personal purposes, processing additional compensation to his own payroll and to other employees, adding extra unauthorized amounts to his own retirement account and to that of other employees, processing large wire transfers to women in China, and transporting cash withdrawn from WM's operating account on his trips to China. David reported that he had accumulated a significant amount of company funds in bank accounts he established in China. His ultimate plan was to travel to China one last time and never return.

Armed with the evidence, Harold set out to recover as much of the $1.8 million as possible. He seized David's assets, liquidating them to generate funds. Combined with funds returned by David and proceeds from an insurance claim, Harold recovered close to $1.2 million for his company. WM prevailed in a civil judgment against David. He was also convicted of first-degree larceny and sentenced to more than five years in prison.

While you could say that this has a somewhat happy ending for the company in that it recovered a large portion of the stolen funds and won a criminal conviction, the company might have been able to avoid being victimized if it had better internal controls. The following are steps that any company can take to prevent embezzlement or detect it sooner. Also discussed is how a company can reduce any loss through proper insurance coverage.

Prevention

Prevention begins before the employee is hired. The goal is to screen out those with a history of stealing from prior employers. Embezzlers will try to throw the company off track by masking their name, past employers, or other information that might reveal past misdeeds. Companies should carefully screen all new hires for any anomalies.

The next step in prevention is to monitor existing employees' behavior for signs of potential theft. In my experience, most victimized organizations interviewed after the scams have come to light describe actions, behavior, and lifestyle issues of the embezzler that could have led to the discovery of employee theft had they been noted earlier. One example is if the person appears to be living beyond his or her means.

While ongoing screening may not be necessary, companies should consider conducting background updates if red flags appear in an employee's behavior. For example, David's practice of leaving during the day for long periods and his frequent trips "to Florida" to help his elderly parents might have been red flags.

Detection

Employers must implement and maintain internal controls and segregation of duties. If the person has access to company accounts, there should be a system of checks and balances, with other people reviewing the accounts.

In today's business environment, all employees, including those in finance departments, perform more functions with fewer resources. However, companies can achieve practical controls using existing resources by simply reengineering the financial processes. Companies must involve individuals who typically would not be part of the process, such as engaging a different person to mail out signed checks directly to vendors, rather than returning those checks to the very same individuals who make purchases and process payments.

Many organizations lack the obvious control of having different people handle different aspects of the company's finances; for example, one person should be generating checks and making deposits while another should be receiving, opening, and reviewing the bank statements. In the WM case, someone other than David should have been receiving, opening, and reviewing the bank statements each month. This would have revealed the fraud or prevented him from even attempting it.

While auditors (internal or external) can't necessarily detect frauds, they can prove invaluable in independently and objectively reviewing the system of internal controls and accounting procedures.

Insurance

With prevention and detection comprising two corners, the third corner of the antifraud triangle is to obtain and maintain appropriate insurance.

The applicable coverage, typically a component of the commercial insurance policy as a rider or add-on, is commonly referred to as employee crime, employee theft, or employee dishonesty insurance. While coverage will provide a means to recover stolen funds, the victim often has to incur costs in the form of professional fees to investigate the loss and submit a claim. Therefore, the company should ask whether, in addition to covering the loss amount, the policy also covers the cost of the investigation into the crime.

This type of coverage is based on a claim event, meaning that one embezzlement scheme is one claim. And a company must decide how high the coverage amount will be. The higher the coverage, of course, the higher the cost, but more and more entities are buying coverage that is for hundreds of thousands of dollars.

An embezzler can be anyone from a volunteer to a senior executive. And it is estimated that only one in nine is actually caught. However, by taking the right steps, companies can improve their odds of preventing or detecting any attempt to siphon off corporate funds. ■

Stephen Pedneault, CPA, CFF (Certified in Financial Forensics), CFE (Certified Fraud Examiner), is principal of Forensic Accounting Services, LLC, in Glastonbury, Connecticut.