WHITE-COLLAR CRIME FIGHTER
YOUR SECRET WEAPON IN THE WAR ON FRAUD
www.wccfighter.com

Gary Zeune, *The Pros and the Cons*

How to Predict When People Will Embezzle

...and How to Stop Them

Usually, three things must be present before someone commits fraud or embezzles…

- Need.
- Opportunity.
- Rationalization.

I call this the "triangle of fraud".

The formula sounds simple, but when you think about the elements of each of the three triangle parts, the picture becomes a bit complex. The following guidelines may help…

THE NEED FACTOR

Need takes two forms—direct and indirect. Direct need involves stealing to resolve a desperate financial problem.

Direct need is often driven by an addiction or compulsion—drugs, alcohol, gambling or an extramarital affair.

Indirect need, on the other hand, is a business owner's or executive's need. It typically is the need to keep the company afloat. This need results, for example, in cooking the books to make sure a loan is obtained or renewed—to buy time to fix a dire financial problem.

Of course, it can also result in a host of other fraudulent acts, such as bank fraud, check fraud, invoice scams, etc.

THE OPPORTUNITY FACTOR

Opportunity is defined as a perception that there is a low probability of being caught. In accounting, the descriptive word for this is "poor internal controls."

THE RATIONALIZATION FACTOR

Rationalization is the employees' mental process of making his or her illegal action fit within a personal code of conduct or ethics. In other words, the dishonest employee must be able to "talk himself into the action."

Rationalization often results in what I refer to as "situational fraud." Employees' propensity to steal or embezzle can be predicted on the basis of a widely accepted formula: 5% to 10% of employees would never—ever—do anything wrong. Another 5% to 10% of employees are always scheming (hopefully you don't have many of these folks working for you). The real problem is the 80% to 90% of remaining employees who will commit "situational fraud"—fraud that results from being in a position to steal and easily rationalize the illegal deed.

Remember: Who are the only employees who can steal from you? *Answer:* Employees you trust. This isn't meant to imply that you shouldn't trust employees. It simply means that you can't afford to go lax on internal controls because you trust employees. Here are some warning signs and conditions where trusted employees may be tempted to commit situational fraud:

- A period when the organization is being downsized.
- Employees who are bored may steal for excitement.
- Employees make an honest mistake, discover a weakness in internal controls, benefit from it and are going to "pay it back."
- Thrill-seekers who like bending the rules when the right situation presents itself.
- Employees who are under personal stress—with financial problems, divorce, serious illness (especially of a spouse, parent or child).
- Employees with addictions—to drugs, alcohol, extramarital affairs, gambling, etc.
- Employees who always have to be number one and/or can't stand not being the center of attention

ANTICIPATING CRIME

Modern CFOs know a lot about human behavior. For example, they know that behavior never remains static. World-class CFOs understand that any time they change a reward, the compensation system or the control system, people will change their behavior to maximize the benefits of the change for themselves.

Example: Many years ago automobile traffic engineers set out to reduce the accident rates at intersections. They set up cameras and videotaped the traffic patterns. At that time, the green light would turn red and the red light would turn green at the same time. But that one last car tried to get through while cars with the green light had permission to go. So the engineers changed the sequence to add a two- or three-second delay (i.e., both lights stay red for that brief moment), giving that one last car time to go safely through the intersection. And of course adding the amber light soon became the standard for creating this delay.

The accident rate declined significantly for two or three months. Then what happened? Drivers coming to an intersection with a yellow light or just-changed-to-red light realized they had several extra seconds to make it through the intersection. Instead of one car going through on the red, now it's three or four. The drivers adjusted their behavior to benefit themselves.

How does this apply to employee theft? When you change a system, policy or procedure, employees will change their behavior—sometimes in a dishonest way. You may solve one problem, but create an even worse problem.

You can't afford to go lax on internal controls because you trust employees

So, what's the solution? A sports metaphor may explain. Hockey players don't skate to where the puck is, they skate to where the puck is going to be. So —to become effective at managing change without promoting crime, you must anticipate how employees—and executives—will react dishonestly to any changes, and correct for them.

MINIMIZING FRAUD

Sometimes vulnerability to employee theft can be reduced with a little creativity. *Examples:*

- The owner of a small company with little segregation of duties can have the bank statement sent to his or her home, not to the company. To demonstrate his attention to the statements, the owner reviews them and then inquires about several items in each statement. This practice creates the perception that a theft would probably be detected, thus reducing the "opportunity" by increasing the risk of getting caught.
- Employees in a large company's purchasing department may set up phony vendor accounts with their own addresses. To deter this kind of theft, regularly match the employee address file with the vendor address file.
- Send a letter to banks where the company does business, asking to keep you informed whenever they open accounts using names similar to that of your company. If someone is stealing customer checks from AT&T, they might open an account under A&TT. The teller would likely accept the check for deposit assuming the company's customer simply wrote AT&T incorrectly.

Important: If you are an outsider—an accountant, auditor, banker, etc.—be aware that you may need to "sell" the importance of fraud deterrents from the bottom up…especially in small companies. Few business owners are eager to implement controls, because they don't want to send the message that employees aren't trusted any more.

The solution: Get one of the company's own employees—the bookkeeper or controller, for example—to ask for the change. Say, "You know, you have complete control of everything. You pay the bills, you make the bank deposits and you reconcile the accounts. If any money is missing, who do you think Sally (the owner) will suspect? For your own protection, you should get Sally to look at the bank statements and initial the envelope every month. I know she's busy, but it won't take her more than five or 10 minutes."

CONCLUSION

Business owners and CFOs must be aggressive about protecting the company's assets. You must understand how your internal controls, compensation and performance measurement systems drive employee behavior and structure these systems so that they keep the triangle of fraud in check.

Source:

Gary Zeune, CEO, The Pros and the Cons, the only speakers bureau in the US for white-collar criminals. He has authored several books, including *The CEO's Complete Guide to Committing Fraud*. gzfraud@bigfoot.com.