

THE FRAUD CLINIC

by Tim J. Leech, CA, MBA

Learning to Think Like a Criminal

I am sure that most of you have heard the expression "It takes a thief to catch a thief". This month's column discusses how to train fraud auditors to think like people who perpetrate frauds. I believe that, if auditors are to be successful detecting and preventing fraud, they must be trained to answer a fundamental question: "If I wanted to defraud this organization, how could I do it?"

Thinking like a thief

A number of years ago, the need to take this approach was emphatically driven home to me as the newly appointed Manager of Special Audit Services for a major oil and gas company. One of my primary responsibilities was to prevent and detect the theft of crude oil from our oil production facilities and from facilities of other companies where we had an ownership interest.

Apparently, many experienced oil company personnel didn't believe that crude oil theft was a possibility, let alone a serious concern. Their position was, "Even if somebody wanted to steal crude oil, what would they do with it?"

So that I could be ready for them and think like an oil thief, I took the following training in oil patch criminology:

- Joined the Petroleum Industry Security Council, a Texas based association set up to combat oil theft and oil field crime.
- Attended the International School of Hydrocarbon Measurement in Norman, Oklahoma.
- Studied an industry text entitled Investigating the Oil Patch, published by the United Petroleum Security Cooperative.
- Spent considerable time and effort in social establishments (known as bars) learning the intricacies of oil field detective work.

- Researched known cases of crude oil theft and discussed these cases with law enforcement personnel.
- Completed oil and gas technology training and training in oil and gas regulatory frameworks.
- Spent many hours thinking how I could defraud my company (strictly for professional reasons, of course).

If auditors are to be successful detecting and preventing fraud, they must be trained to answer a fundamental question: "If I wanted to defraud this organization, how could I do it?"

In your industry, I'm sure that there are comparable training opportunities, reference texts and practical situations to be explored. It can work for you as it did for me. I learned

that one of the answers to the question of how crude oil could be stolen was as simple as the following.

Buy an oil well that is a marginal producer. Get a truck. Drive up to a number of oil wells each night and steal a few barrels from each. Pump the oil down your well. "Produce" the oil. Pay the royalties, sell the oil and collect the revenue. This is simple, effective, hard to detect, lucrative and, most important, not even visualized as a possibility in the minds of the rightful owners of the oil. Scams of this type have gone on undetected for years -- both in the U.S. and Canada.

Many other ways of stealing oil were uncovered during my self-created oil patch criminology program. Many of these had the potential to rob oil companies of millions of dollars, with limited risk to the perpetrators. Only by educating myself and the managers responsible for these sites could our officers be confident that the company was effectively managing risk in this area.

This should be a valuable lesson for your department. To anticipate what frauds could be perpetrated, you have to try to think like the perpetrator. Depending on your industry, you may want to consider taking courses or conference sessions on potential frauds in your industry. You must understand not only the basic, generic fraud methods, but also the techniques specific to your industry.

Assessing the management team

Once you understand the methods, you must assess your management team to determine whether it is "street wise" to the risks that your organization faces. If your assessment (which is more likely to be informal rather than formal) indicates that the management team is in fraud techniques grade school when your opponents have a masters degree, you must take steps to help your company equal the odds. You may want to conduct industry crime workshops for your management teams. This is an excellent project for the audit and security departments to sponsor jointly.

Right about now, you may be saying to yourself, "Wait a minute. Isn't there a risk that by training your staff on fraud techniques you will be slitting your own throat?"

Quite the contrary. In my experience, the dishonest people already know how to defraud companies and are getting better at it every year. It is the honest people, many of whom manage your organizations, who haven't given much thought to cheating and stealing. As a result, the dishonest people can reap large benefits because of the handicaps of the honest people, such as their beliefs that:

- Their staff wouldn't steal from them.
- Their staff wouldn't know how to defraud them.
- Control systems would defend against a material fraud.
- Long-time staff are all loyal to the company.
- Fraud may be happening in the industry or in our organization, but it certainly isn't happening in my department.
- Senior people have too much at stake to risk stealing from the company.
- Segregation of duties is always effective as a fraud prevention/detection control.
- The manager of the area would catch any fraud that was taking place.

The list could be extended, but even this points out that one of the key steps to any effective fraud detection and prevention program is to ensure that staff are sensitive to fraud and alert to possible signs.

This article originally appeared in the June 1990 issue of The Bottom Line.

Some industries are more advanced than others. The retail trade recognized and acknowledged some years ago that the biggest risk it faces is its own staff. Very few other industries have taken the same amount of time to educate their staff on the sinister side of life.

Evening the odds

What can you do, as internal auditor, to even the odds? Here are some ideas:

- Take basic and advanced fraud prevention and detection training.
- Ensure that your management team is street wise to fraud related risks.
- Belong to organizations like the Institute of Internal Auditors and the National Association of Certified Fraud Examiners.
- Subscribe to journals concentrating on fraud, such as Computer Fraud & Security, EDPACS The EDP Audit, Control and Security Newsletter and this newsletter.
- Search out industry-specific sources. The banking industry has a fraud prevention/detection newsletter; the insurance industry has the International Association of Insurance Fraud Agencies; the retail trade has a loss prevention group in the Retail Council of Canada, the oil patch has the Petroleum Industry Security Council; and, for general reference, the American Societies of Industrial Security provide useful information exchange forums.
- Attend fraud-specific training and information exchange conferences.
- Read up on fraud. There are a number of excellent texts on fraud prevention and detection.

I believe that all auditors should have a high level of fraud awareness. If you are to fully support your management team, your knowledge level and skill should allow you to compete on even ground with those who wish to defraud your organization.

At the time this article was written in 1990 Tim Leech was Managing Director of NCM Control & Security Services Limited, the Canadian subsidiary of an international consulting firm based in London, England. Tim Leech is now Principal Consultant and Chief Methodology Officer at Paisley Consulting, a world leader in business accountability software solutions. He can be reached by phone at 905 823 5518 or by email at tim.leech@paisleyconsulting.com