Preventing fraud starts with thinking ahead

By IAN HARVEY

Chances are more than 80 per cent of your employees would steal from you given the opportunity, according to forensic accountant Bashir Rahemtulla.

"They say 20 per cent of your employees can't wait to steal from you, 20 per cent would never steal from you and 60 per cent would if they could," Rahemtulla, president of Intelysis Corp., said at the CGA 2014 Controllers' Congress in Mississauga, Ont. "In my experience it's more like 10 per cent plus 10 per cent and 80 per cent."

The other acronym for fraud is GONE, he said — Greed, Opportunity, Need and Expectation, the latter meaning they don't expect to get caught.

Stopping fraud before it starts is a better strategy than trying to root it out and find the guilty parties once it's happened, he said, noting every manager and financial officer must be vigilant and put aside personal biases in ensuring red flags on accounts are properly investigated and followed up.

Better yet, he said, put processes and controls in place before it starts.

The triggers for fraud in the workplace are well documented going back to the 1950s, when sociologist Donald Cressey created his theory of the three elements always present in the "fraud triangle" —pressure, opportunity, and rationalization.

"It could be personal failures, business failures, personal isolation, the pressure to gain status," he said, noting that the opportunity usually revolves around being in a position of trust and rationalization completes the loop. "They say, 'oh, I'm just going to do it once' or 'I'm just borrowing' or 'they owe me' or 'I deserve this.'"

Never rule out greed as the overriding factor, though, he said: "Of course the first flag in fraud is looking at your employees' lifestyle. Look and see if there's a red Ferrari in the parking lot."

All kidding aside, it's not always that simple because fraudsters aren't that stupid, he added quickly, telling a story about an investigation into a bookkeeper who raised suspicions when she announced she was going on a $5,000 vacation to Hawaii.

"We checked and it turned out her boyfriend, who she hadn't talked much about, was putting up the money," said Rahemtulla, a CA, CPA and CFE who opened Intelysis about 17 years ago and serves a global client base.

In reality the onus is always going to be on the company and its management team to watch for fraud and investigate it. For the most part, police aren't interested.

"Unless it's a granny being defrauded out of their life savings they really don't want to bother," he said. "Maybe if you do all the investigation and wrap it up with a bow and take it to them, they might act."

"It could be personal failures, business failures, personal isolation, the pressure to gain status [which drives the pressure]."

Bashir Rahemtulla, Intelysis Corp.

Generally, he said, U.S.-based companies want jail time, which isn't always easy given the lack of police interest. In Canada they want to terminate quickly, recover the money and move on.

Most frauds are fairly simple and usually leave a trail a decent forensic auditor can pick up on;

RAHEMTULLA

Generally, men steal more in bold schemes while women take less in a series of more actions.

Enron, for example, was a complex, massive-scale fraud involving a series of shell companies with bad assets buried and other assets overstated or simply fraudulently classified. The victim wasn't the company as such — though it folded — but the shareholders, whose stock plummeted from $75 to zero when the ruse was discovered.

"They were enriching themselves with bonuses tied to the stock price," Rahemtulla said.

Such large-scale fraud isn't unusual. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), a thought-leadership organization in the U.S., looked at 347 public company frauds over 20 years from 1998 to 2007 accounting for some $120 billion in misappropriated funds, though Enron and WorldCom skewed the numbers because they were so outrageously large. It found the CEO and/or CFO was complicit in at least some level of participation in 89 per cent of the cases. They also found that within two years of a Securities and Exchange Commission investigation, some 20 per cent of CEOs/CFOs had been indicted and over 60 per cent of those indicted were convicted.

"Of course the first flag in fraud is looking at your employees' lifestyle. Look and see if there's a red Ferrari in the parking lot."

Bashir Rahemtulla, Intelysis Corp.

Enron was similar in that it was an accounting fraud designed to cover the company's real expenses and revenues and make margins seem more attractive to pump the stock price. One of the patterns Enron used was to reduce reserves, with management signing off to the auditors that the funds "were no longer required."

Satisfied, the auditors didn't question the logic of such decisions, or others such as $500 million of computers that were in one case shifted from being a capital expense to an asset, for example.

It was similar, albeit on a smaller scale, to a fraud he encountered at a Canadian computer company which had about $100 million a year in sales but a profit margin of only $2 million.

"That's how paper-thin margins are in the computer industry," he said.

The company had millions in a warranty-provision reserve fund but wrote it down, saying they didn't really need the money because generally the products failed only within the first 90 days and they could easily handle those repairs from cash flow.

"I was acting for (a prospective lender) and we investigated further and found warranty invoices showed computers were failing a year into a two-year warranty," he said. "My client walked away but another lender stepped up. Six months later the company folded."

In most of the cases he sees, the common theme is a lack of internal controls, with managers delegating sensitive tasks to "trusted" employees, like the CFO who gave his secretary his password and had her enter and set up approved vendors.

"It was very hard to become an approved vendor but once approved all invoices would be paid without question," said Rahemtulla. "But she set up her brother-in-law as a vendor."

It usually comes down to trusted employees, he said. He finds that when he identifies the culprit in his investigations the company managers recoil in disbelief and horror citing the suspect "as our best employee" or "my friend" or "most trusted person we have."

Tighter controls and more cameras in retail stores and warehouses, along with some basic common sense, usually stops internal theft at the floor level, he said.

At the executive level, legislation in the U.S. such as *Sarbanes-Oxley* in reaction to WorldCom and Enron have tightened things up, he said, creating and strengthening corporate controls, requiring enhanced financial disclosures and setting new standards for corporate accountability, along with new penalties.

Companies now have to "dig deep to examine the effectiveness of their control but it's very time-consuming and a drain on manpower."

For private companies and those which don't have to comply with *Sarbanes-Oxley*, internal controls are the better options, pointing to the COSO Internal Control — Integrated Framework (at www.coso.org) as a good template. He said it's efficient, reliable and effective, but stressed it's a process which in the end relies on people more than manuals and policy statements.

Most important is ongoing action to control the environment, assess risks constantly, develop a matrix and control activities related to those risks, gather relevant information and clearly communicate internally and externally where needed.

Finally, Rahemtulla said, monitoring is critical to ascertain whether the controls in place are working effectively.