

Fraudsters hit small business: Shareholders at risk: As much as 6% of revenue is lost each year

Financial Post (National Post)
F 10'03

Page: BE1, BE5

Byline: Paul Barker

Source: The Canadian Index (Business)

Full Text: Yes

Idnumber: 200302100205

Subject: Small business; Canada; Forensic accounting; Employees -- Fraud
Version: CBCA: Fulltext Business; CBCA: Fulltext Reference; CBCA: Index
Feature: Illustrations

It was almost the perfect crime.

In the late 1990s, the chief executive of an Ontario manufacturer with annual sales of \$60-million brought in an outside forensic team to go over the books.

The alert CEO was concerned about the company's accounting -- with good reason. It turned out the company's chief financial officer, who also happened to oversee all information technology systems at the company, had been electronically siphoning funds for the past five years.

Had an external financial audit not taken place, she might still be building her little nest egg, which investigators calculate reached close to \$5-million before she was finally caught.

Corporate fraud such as this is so rampant across North America, it is estimated as much as 6% of a company's annual revenues will be lost to inside and outside crooks skilled in corruption, embezzlement and misappropriation of assets.

The Association of Certified Fraud Examiners, a U.S.-based organization with nine chapters across Canada, estimates the majority of perpetrators get away with pilfering for at least 18 months and small businesses are the most vulnerable to occupation fraud and abuse.

According to KPMG Forensic, the people carrying out fraud can be a business's employees, former employees, suppliers, investors, customers, business partners, or sometimes even competitors.

KPMG Forensic says people typically view a fraud perpetrator as a solitary embezzler, someone who is fudging an expense report or someone who is systematically stealing to support a drug or gambling addiction. Much more serious matters hit the front page of late, however.

In its most recent Fraud and Misconduct Diagnostic survey, the company said the alleged manipulation of financial statements by executives at Enron, WorldCom and others has moved the issue of fraud closer to centre stage.

Derek Rostant, president of KPMG Forensic, gives corporate Canada a B grade for its attempts to

prevent fraud, a mark he describes as no longer acceptable. The results suggest Canadian businesses need to be more vigilant and protect themselves and shareholders from the risk of fraud and misconduct, he said.

Criminals, the company says, are keeping up with the times and making the most of technology to divert funds electronically, launder money and steal information. The world of e-commerce is also "changing the way we do business and providing a whole new arena for crime."

The onus now is on organizations of all sizes to keep up with the times. Stephen Hollander, economic crime section coordinator with the B.C. Institute of Technology's forensic science technology program, says the majority of losses are both predictable and preventable.

Preventive measures are not magic, they're just common sense, says Mr. Hollander who trains economic crime watchdogs. "If you're losing 6% of your gross to fraud, you are going to want to get some of that back," he says. "If you wanted to talk about auditing control two years ago, it would have been considered a pencil-neck geek issue. These kinds of issues are now being discussed by board members and we're seeing the doors open more to these concerns."

Last month, BCIT and KPMG Forensic launched a 13-week online course designed to provide executives with the skills needed to recover stolen business assets. Course instructor Gary Gill, senior vice-president with KPMG Forensic, says while the task of recovering what was lost often appears monumental, with the right knowledge and skills, recovery of some, if not all, of the assets is often possible -- if a company knows where to look and what to do.

Software advancements such as data mining and data extraction tools, which examine and analyze data stored in a database, can be a company's biggest ally in fighting fraud.

"You can use data mining to identify patterns of activity in a customer's account," Mr. Hollander says. "You don't have to wait until the customer has swindled you and put the money overseas. What it does is give you a red flag so that you can take

precautionary measures."

John Verver, vice-president of professional services at ACL Services Ltd., a Vancouver company that bills itself as the "market leader" in data extraction and analysis tools and fraud detection and prevention, says organizations in the past have tended not to use technology to look for fraud.

"Systems would have to perform such complex analysis to detect and prevent every type of fraud that it would actually slow down the operation of a business," he says.

"The important thing now is having technology that can independently monitor transaction and provide rapid feedback when you have something suspect."

For small to mid-sized businesses, one of the most common types of fraud, he says, revolves around the "phantom" vendor, in which an employee sets up a "dummy" company as a supplier and has cheques sent to a post office box or into a bank account. Software now exists that will look for matches between vendor names, bank accounts and addresses and the bank account numbers and addresses of employees.

Mr. Hollander says increasingly the private sector is turning to technology rather than running to the police to obtain redress from economic crime.

The key, adds Mr. Verver, is having the ability to quickly catch a transaction gone bad and respond quickly.

"We're at a point now where people responsible for control, audit and fraud detection are suddenly realizing that software exists that allows them to be pro-active, instead of reactive," he says.

Copyright 2003, Financial Post from National Post (formerly the Financial Post Company). All rights reserved.