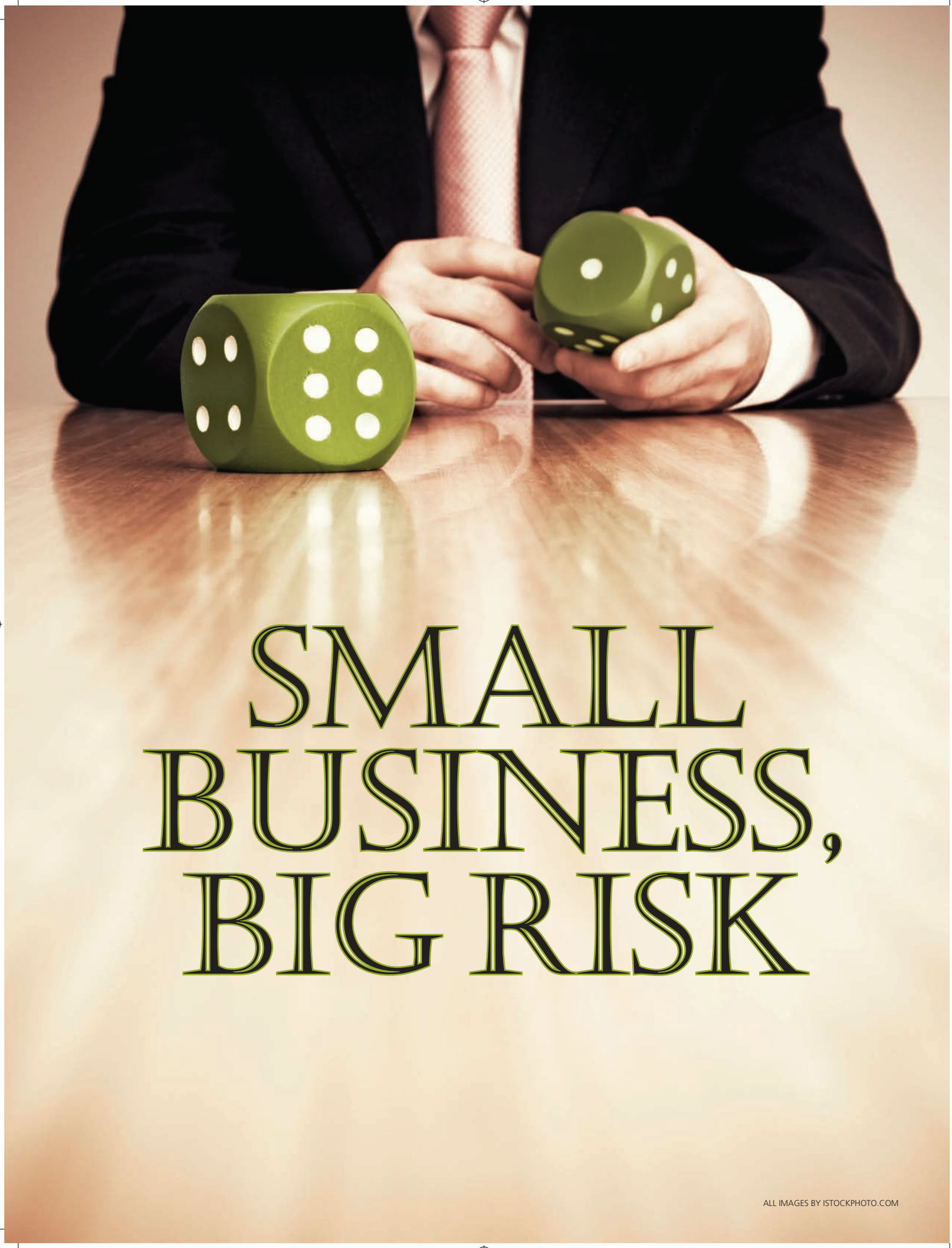

# SMALL BUSINESS, BIG RISK

ALL IMAGES BY ISTOCKPHOTO.COM

# Fighting fraud no simple task in an environment that includes fewer internal controls

## / By CHRISTOPHER GULY

**THE COST OF** doing business shouldn't involve theft — but it does.

A typical organization loses five per cent of its revenues annually, or nearly $3.7 trillion to fraud (all figures U.S.), according to the results of a global online survey of 34,615 certified fraud examiners last year by the Texas-based Association of Certified Fraud Examiners. Hardest hit with the highest incidence of victimization of 29 per cent were organizations with fewer than 100 employees, which reported a median loss of $154,000.

"Small businesses are both disproportionately victimized by fraud and notably under-protected by anti-fraud controls, a combination that makes them significantly vulnerable to this threat," said the report. "While resources available for fraud protection and detection measures are limited in many small companies, several anti-fraud controls — such as an anti-fraud policy, formal management review procedures and anti-fraud training for staff members — can be enacted with little direct financial outlay and thus provide a cost-effective investment for protecting these organizations from fraud."

Toronto chartered professional accountant Patricia Harris, who often conducts forensic accounting investigations at small businesses, says that owners sometimes get the ball rolling.

She recalls that in one case, a business owner had a "Spidey sense" something wasn't quite right with bookkeeping, and enlisted Harris and her team to do some test sampling. They discovered internal controls needed some improvement and recommended a sharing of duties regarding vendor payments.

"There was no fraud, but the owner felt there were some weaknesses, and he was right," says Harris, a partner with the chartered professional accounting and business advisory firm Fuller Landau.

The ACFE study found that seven per cent of fraud cases were detected by accident. Harris says that business owners typically don't find such scams. More commonly, they're uncovered by whistleblowers within a company.

"Unfortunately, they're not treated as the heroes they or we think they should be and are seen more as troublemakers — especially if they're whistleblowing on a highly trusted employee," says Harris, who witnessed this firsthand in a case in which an employee approached management about possible fraudulent activity by a 30-year employee within the same organization.

"They made the whistleblower feel she didn't have her facts straight, but when we investigated, we found there had been a misappropriation of funds. When somebody speaks up, they need to be taken seriously."

The ACFE study found that tips were the most common detection method, accounting for four in 10 cases, or more than twice the rate of any other detection method. Employees accounted for nearly half of all tips that led to the discovery of fraud.

They also commit most (42 per cent) of occupational frauds,

according to the ACFE study. And 82 per cent of fraudsters are first-time offenders who had not previously been punished or fired for fraud-related conduct.

"Most fraudsters work for their employers for years before they begin to steal," says the report.

Certified fraud examiner Jim Muccilli, a partner in the valuations, forensics and litigation group at Toronto-based accounting firm Crowe Soberman, says that employee theft is often initiated based on opportunity, not need.

"They'll start small, such as stealing from petty cash, because it looks easy. And once they see they haven't been caught, they gain confidence and may begin adding zeros to cheques — so the fraud goes from hundreds of dollars to thousands of dollars."

The occupational fraudsters usually get caught, says Muccilli, when they get "sloppy or greedy," and typically when they're on vacation and someone filling in their role detects anomalies.

Based on his experience, financial statement fraud — which may include recording fictitious revenues, understating reported expenses and/or artificially inflating reported assets — generally triggers the largest losses, often because it originates with upper management and therefore can involve millions of dollars.

"At the end of the day, there is often little left for stakeholders or lenders to recover," Muccilli says.

According to veteran Toronto forensic accountant Edward Nagel, payroll is particularly vulnerable to fraud due to the volume and frequency of transactions that occur throughout the year.

One common scam involves the creation of fictitious or "ghost" employees who usually don't work for the organization, or less commonly, once worked there, including deceased employees. The fraudster, normally a payroll employee who works late or doesn't take holidays, uses the former employee's social insurance number or creates a fake one and arranges to have cheques or direct deposits sent to the ghost at an address or account the fraudster controls.

**"They'll start small, such as stealing from petty cash, because it looks easy. And once they see they haven't been caught, they gain confidence and may begin adding zeros to cheques – so the fraud goes from hundreds of dollars to thousands of dollars.**

Jim Muccilli
Crowe Soberman

Nagel says to detect and prevent this practice organizations can take several steps, such as segregating duties within payroll since many frauds involve collusion. They should also ensure there is a paper trail for all payroll transactions to help trace and recover misappropriated funds, and have someone — preferably outside the payroll function and on a rotating basis — regularly reviewing reports.

"Technology has started to play a greater role in checking for errors and other anomalies, thereby effectively automating this review process," says Nagel.

A prevalent scam involves falsifying expense reports either by including personal expenses as business-related, inflating or duplicating expenses, or obtaining an advance and then claiming an expense against it without reconciling the two.

"If all personnel know their expenses will be closely checked, this inherently can serve as a deterrent for would-be fraudsters," says Nagel. "But even if they continue to perpetrate this type of fraud, the chances of catching it are high with proper monitoring."

The challenge for small companies is that they have fewer internal controls and a lack of segregation of duties, and also have a high level of trust in long-term employees, says Harris. "You may have someone who has accounting authority to set up a vendors list and make payments, which in many cases works fine but really exposes a small business to fraud."

Separation of duties is one solution, she adds. Another is to change passwords regularly to ensure that no one employee always has access to automated financial systems. Ultimately, though, the top control rests with the owner, who should regularly review and monitor the business's banking account, payroll, expense reports and vendors lists, according to Harris.

"They should do a random check every month to see, for example, if any new employees have been added to the payroll — and they should also ask questions, such as why amounts paid on an account vary over a period of time," she says.

Harris points out that one of the more common ways money leaves a business is through a phantom vendor, which may only list a post office box as an address.

"That's why it's important to have a vendor-approval process overseen by the business owner or some other level of management that requires authorization for cheques over a certain dollar amount."

She also recommends that small business owners carefully read financial statements.

"Most will understand revenue and expenses, but they need to look at other aspects, such as accounts receivable.

"If someone who is prone to stealing knows someone is checking, they're less likely to do it — and get away with it."

However, some fraud can be difficult to detect, says Muccilli.

"Fraud created with enough complexity and co-operation among key people in upper management can escape an audit, which is not designed to detect such schemes."

The ACFE survey found that external audits are among "the least effective controls in combating occupational fraud" and were the primary detection method in just three per cent of fraud cases reported. Yet "the most effective anti-fraud controls

are being overlooked by a significant portion of organizations."

For example, only 35 per cent of organizations relied on proactive data monitoring and analysis despite this control correlating with frauds that were 60 per cent less costly and 50 per cent shorter in duration.

The ACFE report also indicates that employees working in one of seven departments — accounting, operations, sales, executive/upper management, customer service, purchasing and finance — committed more than three-quarters (77 per cent) of the frauds in the study.

Recovering stolen money is also a challenge: 58 per cent of the victim organizations in ACFE's study had not recouped any of their losses due to fraud, and only 14 per cent had made a full recovery.

Not surprisingly, the ACFE concluded the longer frauds last, the more financial damage they cause, particularly since passive detection methods such as confessions, notification by law enforcement, external audits and accidental discovery "tend to take longer to bring fraud to management's attention," says the report. "Consequently, proactive detection measures — such as hotlines, management review procedures, internal audits and employee monitoring mechanisms — are vital in catching frauds early and limiting their losses."

There is also a way of catching occupational fraudsters, says the report. They exhibit certain behavioural traits — "such as living beyond their means or having unusually close associations with vendors or customers" that can serve as "warning signs" of their crimes. (The ACFE study found that in 92 per cent of the cases reviewed, at least one red flag — which include experiencing financial difficulties and unwillingness to share duties — was identified before the fraud was detected.)

But while the causes and effects of occupational fraud may seem complicated, small business owners should remember a simple strategy, offers Harris. "If you have ongoing employee monitoring and an understanding of the risk factors and warning signs of fraud, you are much more likely to identify it and stop it."



ALL IMAGES BY ISTOCKPHOTO.COM