JOSH RINEHULTS/GETTY IMAGES/ISTOCKPHOTO

JORDANA DIVON
SPECIAL TO THE GLOBE AND MAIL
PUBLISHED NOVEMBER 26, 2012
UPDATED APRIL 2, 2018

When a small retailer approached him with suspicions that an employee was stealing cash, Randy Nelson, president of PROAM Civil Recovery and Security Solutions, a Mississauga, Ont.-based private-investigation and security company, set up surveillance cameras throughout the firm's three locations.

He monitored the company for a month before zeroing in on one employee. The staffer eventually confessed to stealing $60,000 over two years, and was charged and convicted, he says.

Though the company received partial restitution, Mr. Nelson says the emotional fallout was even more devastating than the financial losses.

"The owners said, 'How could this person do this to us?' " says Mr. Nelson, who got his start in the police force and is also a former national director of loss prevention for companies including Blockbuster Canada and Athlete's World**.**

That company was not alone. Recent reports suggest that employee theft has become a growing problem for small- and medium-sized businesses, with serious results that can harm companies not only financially but also take a toll on their relationships with clients and employees.

Small businesses can suffer big consequences: A 2010 report by TD Bank Financial Group estimated that employee theft played a role in the bankruptcy of one out of 10 failed small- to medium-sized businesses.

Employees are behind a third of the annual $4-billion that Canadian retailers are losing to shrinkage, including theft, estimated a recent study by PricewaterhouseCoopers LLP and the Retail Council of Canada. Moreover, that proportion is up significantly from the 19 per cent attributed to employees in 2008, the study found.

Another 2011 study by the Certified General Accountants Association of Canada found that at least one quarter – 26 per cent – of Canadian small- and mid-sized firms had been the victims of at least one instance of workplace fraud the previous year, losing at least a collective $3.2-billion. The most common types of fraud were "misappropriations" of inventory, assets and cash, the report highlights noted.

Many small businesses "operate on a small budget and smaller margins… [so] the ability to control shrinkage or theft can often be the difference between being able to turn a profit and going out of business," says Alexander Fernandes, chief executive officer of Avigilon Corp., a high-definition surveillance company based in Vancouver.

What motivates employees to steal in rising numbers?

Stephen O'Keefe, vice-president of operations for the Retail Council of Canada, says that employee theft often boils down to "need, greed or opportunity."

The risk is likely to rise in a slower economy, the CGA report noted, as employees face more financial difficulties.

The holiday season can drive financially strapped employees to top up their funds with a little extra from company coffers, he says.

Employees may also be driven to undermine their employers if they feel underappreciated, says Eduard Goodman, chief privacy officer at Identity Theft 911 LLC in Scottsdale, Ariz.

And many small businesses might unwittingly help to bring on the problem themselves with lax internal policies and procedures and by failing to perform sufficient background checks on staff, Mr. Goodman and the PwC/Retail Council report suggest.

The CGA study estimated that more than 80 per cent of SMEs reported losses of up to $5,000, encompassing everything from pilfered office supplies to pinched client contacts to stolen digital data.

Mr. Goodman deals with companies trying to restore stolen client data that includes highly sensitive medical records, social insurance numbers and credit-card details.

Many security breaches, he says, come from a staff member with direct access to the information – which they can use in the lucrative business of identity theft.

The fallout from these breaches can be far-reaching, as clients may abandon a business in search of more secure pastures, he says.

"You're probably going to have an inherent distrust [of the company] and you're probably not going to want to go back. There are other choices out there," Mr. Goodman says.

Rock Lefebvre, vice-president of research and standards at CGA-Canada, describes costs as "reputational collateral," which can have a devastating effect on both clients and staff.

Smaller companies tend to foster a tight-knit environment, so when a fellow employee steals, other staff can feel as though they've been robbed as well, he says.

In fact, some SMEs reported that the biggest cost to them is how it affects morale, confidence, and loyalty, Mr. Lefebvre adds.

That tight-knit environment is also a reason so much internal fraud goes undetected. The CGA study found that 80 per cent of small and mid-sized business owners were unprepared to respond to employee theft, while 74 per cent believed their exposure to occupational theft was low.

"You would never think that it's your loyal office administrator or your part-time bookkeeper because you hired them, you retained them, you had what you thought was a relationship of trust, and we don't often revisit that," Mr. Lefebvre says.

"We're told that employees get frustrated with management if they don't act on an alleged fraud. They lose confidence in the company," he adds.

Small businesses can take action to discourage theft from within the ranks.

The first steps Mr. O'Keefe recommends are to do thorough background checks on any potential hires, and to put in place an environment where everyone recognizes that one person's actions could cost everyone their livelihood.

Mr. Goodman advises policies controlling access, making sure that certain information is only available to people who need to know it and that employees are educated on security policies, like not sharing passwords.

Mr. Fernandes maintains that the installation of high-quality intrusion alarms and video surveillance can deter would-be thieves from risking exposure.

Mr. Lefebvre also cautions small businesses not to fall behind on their paperwork, since that creates an exposure risk that may encourage some employees to skim a little extra.

The key, however, Mr. Lefebvre says, is for all business owners to shake off the notion that employee theft could never happen to them.

KEEPING EMPLOYEES HONEST

Here are some suggestions from the experts:

Build awareness

Create an environment where everyone has enough self-preservation to know that one person's actions could cost everyone in the company their livelihood, and that suspicious activity should be reported immediately.