THE HEAVY BURDEN OF LIGHT FINGERS

Trust doesn't keep employees from stealing; prevention does

Chris Daniel used to treat employees like family. That is, until his bookkeeper allegedly swiped $122,000 from his company's coffers, which, he says, nearly put him out of business. To cover the loss, Daniel had to cut his own salary by 25%, lay off five employees in his eight-person operation, and take out a second mortgage on his home. "It's like a marriage breaking up over an infidelity," he says. "I was angry, and deeply hurt."

Unfortunately, what Daniel says happened at his small Charlotte, N. C., advertising firm isn't that rare, except that in his case it resulted in state criminal charges—specifically, larceny by employment. (The bookkeeper, arrested in October, 1995, has not yet entered a plea. Her lawyer declined to comment.)

JIM LUDTKE

BIG BITE. In need of an easy cash fix—or just some way to get back at the boss—a growing number of workers are ripping off their employers these days, according to business security experts. The abuses, which range from looting office supplies to embezzling corporate funds, cost employers 6% of revenues every year, estimates the Association of Certified Fraud Examiners, an Austin (Tex.)-based trade group.

While most experts believe that employee theft is a growing problem for all businesses, smaller companies are more vulnerable to its effects. A Fraud Examiners' study of over 2,000 cases handled by its members found small businesses suffered a median loss of $120,000 per incident. The figure for companies with 10,000 or more employees—firms presumably better able to withstand the loss—was just $6,000 higher.

Obviously, startup operations have fewer resources to protect themselves with. They generally don't screen prospective employees very thoroughly, either. (It has been estimated that 30% of all fraud losses could have been avoided if proper employee background checks had been done.) Nor do most small businesses have sophisticated accounting controls in place.

Privately held companies, for instance, are not required by the Securities & Exchange Commission to prepare an annual audited financial statement, so many small businesses don't hire an outside accountant to review their books at the end of the year. Instead, they let the company bookkeeper do it. "That's almost an open invitation to steal," says Bart M. Schwartz, president of Decision Strategies International, an investigative consulting firm in New York. "Every company needs a third party to monitor the books periodically."

What puts small companies especially at risk, however, is the high level of trust that exists between owners and employees. When Douglas W. Slothower, president and chief executive officer of the National Potato Promotion Board in Denver, first learned that a field representative had falsified accounts and stolen $135,000 from his organization, he didn't want to believe it. "We all knew him. He was well liked. It was devastating. We just didn't understand why he would do this to us," Slothower says. The field rep went to prison after pleading guilty to forgery.

EMPLOYEE FRAUD

Often, small-business owners delegate a lot of responsibility to a chosen few. One employee will frequently handle several different jobs—accounts payable and accounts receivable, for instance—so there is little separation of duties. And that creates more temptation for wrongdoing. "No matter how much you trust your employees, you have to monitor their activities—or at least make employees think that you are," says Thomas W. Golden, who directs

At Your Service

JUST CHECKING: Security measures need not destroy the close-knit family feeling many small businesses strive to maintain

Coopers & Lybrand's litigation and claims practice in Indiana, Ohio, and Kentucky. That might not be as hard it seems. The most feared agency of the government is the Internal Revenue Service, notes Golden, yet less than 1% of individual tax returns are actually audited every year.

Uncovering an employee theft frequently happens by accident. Ron Knight, the owner of a construction business in Gilbert, Ariz., never reviewed his monthly bank statements. He let the bookkeeper do that. But one day when she was out to lunch, he just happened to open the mail. He saw a canceled check for $1,000—made out to her. Knight did some digging and soon learned that his bookkeeper had siphoned $20,000 of the company's money since she had joined the company six months earlier. In August, she pleaded guilty to two counts of theft and was sentenced to a year in jail.

POSITIVE SPIN. Not all cases are that easy. Forensic accountants, fraud examiners, and security consultants can help root out the problem—and the employee masterminding it all—as well as assist with the installation of some safeguards to prevent the crime from recurring. "To uncover a theft in the factory or a store, you might need to place an undercover agent amidst the employees," says Ira Lipman, president of Guardsmark, a security consultant in Memphis, "or install closed-circuit TVs."

One Midwest manufacturer, for example, found company products mysteriously appearing in junkyard sales across the country—at very cheap prices. Management quickly hired a team of experts to monitor employees at its production and distribution centers. Ultimately, that led them to an abandoned warehouse that was stocked with parts stolen from the company—as well as parts lifted from three other manufacturers. The investigation led to criminal charges and convictions.

But will security procedures ruin the close-knit, family feeling that most small businesses strive to maintain? Not necessarily. Obviously, you don't want to create an environment in which employees feel that Big Brother is always watching. But most employees are savvy enough to realize that some checks and balances are standard operating procedure. "People are used to seeing some sort of control," says Anthony J. Ridley, general auditor for Ford Motor Co. and chairman of the Institute of Internal Auditors, a trade organization in Altamonte Springs, Fla. "Even in the supermarket, customers know that when a cashier makes an overring, she can't just correct it. A manager must be called over to sign off on the error."

Business owners can ease employees' suspicions by putting a positive spin on the situation. Don't simply tell employees that you're installing a new accounting or inventory control system in an effort to prevent fraudulent activity. Rather, explain that the need for these tactics has arisen because the company is growing and expanding. "Management needs to convey to employees that these are signs that the company is becoming a player," says Bart Schwartz. "It's another way that you are professionalizing the company."

Owners should touch on the issue of fraud, of course. But don't appeal to an employee's sense of morality. "It never works," says Joseph T. Wells, a former FBI agent and the chairman of the Association of Certified Fraud Examiners. "Tell them how much fraud costs and how it's going to affect their paycheck."

If you use these safeguards after a theft has taken place—which is, after all, when most small businesses jump on the antifraud bandwagon—be sure to speak openly about the situation. You may not want to identify the thief (for legal reasons), but you certainly should tell your staff what happened, says Stephen E. Silver, worldwide managing director of business fraud risk services for Arthur Andersen & Co. Most of them will figure it out for themselves anyway.

And what of the thief? At the very least, the person should be terminated—immediately. Some small businesses press criminal charges, too. Not because they necessarily want to see the culprit do jail time, but because they want their money back.

Still, some owners will never file a police report because court cases take time and money—both of which are in short supply in an entrepreneurial operation. What's more, many small businesses are skittish about getting bad press. Once the situation is made public, they feel it will reflect badly on them in the eyes of their customers, their vendors, even their lenders. Some fear—no matter how guilty the employee is—that it will appear as though management simply wasn't minding the store.

By Barbara Hetzer in New York

Fighting Fraud

ESTABLISH A WRITTEN CODE OF ETHICS. It's management's job to set the tone, not the employee's. Be clear about which uses of company resources you view as theft.

KNOW WHO YOU'RE HIRING. Search criminal records at the courthouse. A credit check can reveal a lot about a person's character and possible financial pressures.

SEPARATE JOB FUNCTIONS. Don't let the person balancing the books write the checks. Rotate jobs. Have an outside accountant review operations periodically.

WATCH OUT FOR IDIOSYNCRASIES. A bookkeeper shouldn't drive a Porsche. Persistent late hours and no vacation are suspicious.

SET UP A HOT LINE. An outside subscriber service like the National Association of Certified Fraud Examiners' ethics line can handle the calls.

EXAMINE THE BANK STATEMENTS. Look for checks made out to the same person repeatedly and payments to unknown vendors.

MOTIVATE EMPLOYEES. Tie a portion of compensation to reducing inventory shrinkage and make sure you haven't built in incentives to cheat.