Internal Threat

Businesses Suffer as Employee Theft Grows

ORGANIZATIONS AROUND the world lose an estimated 5% of their annual revenues to occupational fraud, according to a survey by the Association of Certified Fraud Examiners (ACFE).

The association estimates that U.S. businesses lose some $50 billion a year to employee theft, and that 75% of employees have stolen at least once from their employer — and 37% have stolen at least twice. So, what can your organization do to avoid falling victim? The U.S. Small Business Administration and the ACFE recommend that companies:

Use pre-employment background checks – Basic pre-employment background checks are a good business practice, especially for employees who will be handling cash, high-value merchandise, or have access to sensitive customer or financial data.

Be aware that laws on background checks vary from state to state and if you go too far in your check, you may be in breach of the law and risk being sued. Recently the U.S. Equal Employment Opportunity Commission raised concerns that criminal background checks may disproportionately discriminate against some racial groups.

Check candidate references – Make a practice of calling all references, particularly if they are former employers or supervisors.

If your candidate has a history of fraudulent behavior, then you'll want to know about it before you hand them a job offer.

While some former employers may be loath to tell you anything bad, they will often give you clues in the conversation that the employee may have had some problems.

Implement a fraud hotline – Occupational fraud is far more likely to be detected by a tip than by any other method.

More than 40% of all cases were detected by a tip — with the majority of them coming from employees of the victim organization. There are several providers of hotline services that can help implement an anonymous tip-reporting system for businesses of all sizes and industries.

Conduct regular audits – Regular audits can help you detect theft and fraud and can be a significant deterrent to fraud or criminal activity, because many perpetrators of workplace fraud seize opportunity where weak internal controls exist.

Recognize the signs – Studies show that perpetrators of workplace crime or fraud do so because they are either under pressure, feel underappreciated or perceive that management behavior is unethical or unfair.

Warning Signs

Some of the potential red flags to look out for include:

- Not taking vacations. Many violations are discovered while the perpetrator is on vacation.
- Being overly protective or exclusive about their workspace.
- Employees that prefer to be unsupervised by working after hours or taking work home.
- Financial records sometimes disappearing.
- Unexplained debt.
- An employee living beyond their means.

Set the right management tone — One of the best techniques for preventing and combating employee theft or fraud is to create and communicate a business climate that shows that you take it seriously. You may want to consider:

- Reconciling statements on a regular basis to check for fraudulent activity.
- Holding regular one-on-one review meetings with employees.
- Offering to assist workers who are experiencing stress or difficult times.
- Having an open-door policy that gives employees the opportunity to speak freely and share their concerns about potential violations.
- Creating strong internal controls.
- Requiring employees to take vacations.

You should also treat unusual transactions with suspicion and trust your instincts. ❖

Employee Dishonesty Insurance

Employee dishonesty insurance coverage – sometimes referred to as fidelity bond, crime coverage or crime fidelity insurance – protects a small business employer from a financial loss as a result of fraudulent acts by employees.

The financial loss can be caused by an employee's theft of property, money or securities owned by the small business.