Reduce Your Risk of Occupational Crime

Do you have the proper insurance and crisis plan in place? If not, you may be putting your organization at risk.

By Christopher J. Giovino

Nonprofits are especially vulnerable to occupational crime — theft from within the organization. In an environment where people are bonded by support for a common cause, individuals tend to be more trusting — often to a fault.

The criminal can be anyone from an hourly worker to the organization's top executive. Even the most trusted and respected employees, managers, and executives can turn out to be fraudsters.

The size of the organization doesn't matter: Large and small nonprofits are equally vulnerable to employee crime.

And there's more bad news: Most of these losses are either uninsured or underinsured.

Be Aware of Heightened Risk

Occupational crimes are on the upswing — both in the nonprofit world and among private sector businesses, as well as across government entities. The median loss from occupational crime is $140,000, according to the Association of Certified Fraud Examiners.

Of the perpetrators, 87% are first-time offenders. Almost half of the crimes (46%) are committed by lower-level employees, more than a third by managers, and nearly one in five by top executives. The average cost of an occupational crime by senior management: $485,000.

What might motivate people to steal from their own organization? Sometimes they feel they aren't being recognized or compensated enough for their work. In other cases, crimes are initiated by those with gambling or addiction problems.

Some employees just need cash once or twice to make a bill payment. Over time, it becomes easier to convince themselves that the money won't be missed or that they'll eventually be able to repay it at some point, but they just never get around to it.

Because of their access to funds, many cases of embezzlement involve staff responsible for fiscal controls or expense accounting, including those who have signature/expenditure approval authority. Executive assistants, office managers, and accounting personnel are especially prone to occupational crime.

Trust can be your greatest enemy. Breakdowns often occur when someone in the chain of command who prepares documents for approval by the next level in the hierarchy has gained so much trust that the approving authorities simply "rubber stamp" everything.

If there's a time of year when nonprofits are most vulnerable to occupational crime, it's typically when there's more cash available, as well as when the volume of transactions or paperwork increases. That's usually around the holiday season, when there's an influx of donations, or during fundraising events. Organizations that serve the needy are especially vulnerable when disaster strikes and emergency-relief funds flow out to help victims.

> "Most losses are either uninsured or underinsured."

> "The average cost of senior management crime: $485,000."

Prevention Starts with Admitting Vulnerability

The first step in preventing a crime is admitting that your organization is vulnerable. If you have tight financial controls, you may think you needn't worry. Yes, well-conceived and carefully implemented controls are essential safeguards. But, by themselves, they're not enough. That's because perpetrators know just how to keep what they're doing small enough to fly under controls. Thus, it's difficult to detect occupational crimes before they mushroom into major losses.

Be Ready before Crime Occurs

Once you accept that your organization's financial controls have their limitations, your team can move ahead and develop a comprehensive plan to address your potential exposure. Here are seven steps to consider:

1. SPEAK TO YOUR AUDIT COMMITTEE.

- **Tell your organization's audit committee that you want to include fraud investigation** as part of your annual audit.
- **Be sure your audit committee has one contact person,** and rotate that person frequently.
- **Insist that fraud audit interviews** be thorough.

These precautions will take sensitive and criminal matters out of the purview of senior executives. Executives may be complicit in a fraud and not want the matter to surface. That's why an audit committee and an annual audit by an external accounting firm are so vital.

2. CREATE A SWAT TEAM.

Form a small team of people to create a plan for reducing risk. The team might include, for example:

- **the chief financial officer**
- **a board member** with experience in these matters
- **an attorney**
- **individuals responsible for communications,** human resources, information technology, risk management, and operations.

The team should report to one contact person within the audit committee.

3. CONTACT AN INSURANCE SPECIALIST.

Talk to your insurance company and risk advisor or broker. Discuss what protection you have (or should consider) to address risks. Ask yourself questions such as these:

- **Have you done an exposure value exercise** to determine how much money your organization might lose through occupational crime?
- **Do you have adequate crime insurance?** Crime insurance is your best bet if you hope to recover stolen funds.
- **Does your crime insurance policy include an assessment** of your organization's potential vulnerabilities?
- **Does your policy include a self-assessment checklist** of what you can do to minimize your organization's exposure?
- **Does your policy provide "professional fee" coverage,** which would apply if you need to retain an investigative firm to assist with a matter?
- **What specifics does your crime insurance policy stipulate regarding "notice"** — in terms of reporting a claim to the insurance company as well as to law enforcement authorities. Failure to provide timely notice of a crime or related loss might compromise your coverage and ability to obtain full restitution.

4. DEVELOP TIES WITH LAW ENFORCEMENT.

Know ahead of time which law-enforcement agency you should call in the event of a suspected crime. Often, agencies such as the FBI, police departments, and U.S. Attorney's Office have outreach programs that may be helpful to you. Ask. Having an established relationship with a law enforcement officer may reap dividends in the future.

5. VET PEOPLE BEFORE YOU HIRE THEM.

Review what measures your organization has in place to perform background checks for new hires, especially for those with access to the organization's finances. Roughly 13% of occupational crimes are committed by repeat offenders.

And don't forget to perform credit checks. A person in great debt may find it hard to resist the temptation to steal.

6. EXAMINE YOUR CONTROL SYSTEM.

- **Are there sufficient redundancies** built into your organization's financial controls for cash, petty cash, accounts payable, and receivables?
- **To what extent do your officers, directors, and senior executives have oversight of these functions,** especially if your organization has multiple locations?

7. ASK STAFF TO BE ALERT TO POTENTIAL CRIME.

Give people the tools to report, on an anonymous basis, anything that appears suspicious. Ask yourself:

- **Do you have a mechanism, such as a tip-line, that allows employees to communicate freely?** An anonymous tip-line for staff to report suspected offenders may be the single most important tool you can have to thwart internal crime. The vast majority of occupational crimes are detected through anonymous tips.
- **Have you discussed the Whistle-blower Act with staff?** This act protects people from retaliation for reporting suspected fraud and other illegal activities (see employmentlawgroup.net for more details).
- **Have you educated staff** about the importance of internal policing?

When You Suspect a Crime

If you suspect a crime has taken place, the best first step is to initiate an internal investigation. If you've established a working relationship with law enforcement officers, it makes sense to consult them too. They may be able to offer investigative advice and support.

When you suspect an employee of theft, don't be too quick to say, "You're fired." In most situations, you have more leverage in confronting a current employee than a former one. If your aim is to identify potential accomplices and recover missing funds, investigating a current employee may be in your organization's best interest.

Christopher J. Giovino (chris.giovino@aon.com, 203-762-5052) is director of Crime Claims Preparation, Advocacy and Valuation, Aon Risk Solutions, based in Wilton, Connecticut.

Your Emergency Tool Kit

Lessen your risks with these and other articles from the Society for Nonprofits' Library at www.NonprofitWorld.org/members:

Protecting against Fraud (Vol. 31, No. 5)

Six Ways to Reduce Risk & Comply with the Law (Vol. 25, No. 6)

How to Handle a Crisis (Vol. 12, No. 1)

The Audit Committee: Why You Need One, How to Form One (Vol. 6, No. 6)

What Is the Board's Role in Managing Risk? (Vol. 15, No. 5)

Setting Up a Control System for Your Organization (Vol. 16, No. 3)

Fraud: Discovery and Action (Vol. 25, No. 5)

Risk Management: How to Protect Your Assets (Vol. 26, No. 1)