Are You Breeding the Conditions for Fraud to Occur?

Fraud in nonprofits is alarmingly frequent. Avoid it by shaping a fraud-prevention environment.

By Steven M. Braunstein

After an employee commits workplace fraud, leaders often scratch their heads, wondering why such a stand-up individual would perpetrate such a breach. The truth is that even the most loyal employee – and even a usually honest person – can commit acts that seem unthinkable – if conditions are right.

Why Fraud Happens – & Why It's Predictable

In a recent case, the treasurer of a nonprofit – a dedicated volunteer and a grandmother – handled all financial and administrative tasks for more than 10 years, receiving praise from the organization and community. It wasn't until a vendor complained about an unpaid bill that the nonprofit's secretary found a number of inappropriate checks written out of the organization's checkbook. The treasurer had been making cash withdrawals and spending the money on clothing, airfare, and cable bills. The organization lost more than $250,000.

> "It's important to speak directly to previous employers."

Situations like these are shocking but often predictable. Most fraud happens when three circumstances occur:

- an opportunity
- an incentive
- a rationalization.

If an employee comes across a window of opportunity for fraud during a personal crisis, it will be easier to rationalize the unethical act.

For example, let's say nonprofit employee John has identified a weakness in the system that would allow him to take small amounts of cash unnoticed **(the opportunity)**.

John ignores this weakness for several months, but then his wife loses her job and the family becomes financially vulnerable **(the incentive)**.

John convinces himself that he's underpaid and that the small amounts of money he'll take won't affect the nonprofit **(rationalization)**. Once the rationalization is in place, John is likely to take advantage of the weakness in the system.

Who Can Prevent Fraud?

The best fraud deterrent is a system of controls and procedures that prevent it from occurring in the first place. Three groups contribute to this first line of defense:

> "Even the most trusted employee will commit fraud in certain conditions."

The human resources department should perform criminal and civil background checks, as well as checking references. Since white-collar crime rarely results in charges filed, a history of fraud may not be apparent in a criminal background report. It's important, then, for HR staff to verify former employment and speak directly to previous employers.

The IT security team should create monitoring systems and policies about:

- personal-device usage (mobile phones, laptops, and tablets)
- restricted-access areas
- information sharing.

Front line managers must ensure that the policies are actually being practiced day-to-day. They also need to maintain the proper segregation of financial responsibilities among employees. It may be tempting, after someone has worked at your organization for a long time, to relax these controls. That's exactly where the trouble usually starts.

The Key Ingredient: People's Perceptions

Once the proper systems and policies are in place, nonprofit leaders must take the extra step of *managing the perception* of internal controls. If employees don't understand why such controls are in place, the organizational culture can suffer – creating a perceived "big brother" environment, damaging employee morale, and dampening the entrepreneurial spirit that sustains a nonprofit. The following best practices will help strike a balance between maintaining internal control and fostering a welcoming environment.

1. Make fraud prevention policies transparent. Provide information to all new hires about the function of internal controls. Update employees whenever policies are augmented or changed. Each employee should be able to answer the following questions:

- ***What is the goal*** of the fraud-prevention program?
- ***What specific data*** do monitoring systems collect?
- ***Why are financial responsibilities segregated*** in specific ways?
- ***Why is preventing fraud a priority*** for our nonprofit?

Be up front about the purpose of internal controls, explaining that fraud can quickly throw an organization off course and lead to massive, long-term setbacks.

2. Set the tone at the top. Employees will look to you for cues as they form their perception of your organization's culture. You must:

- ***Be consistent*** in your messages about internal controls.
- ***Demonstrate your own compliance*** publically and often. For example, if your organization requires employees to wear badges for access to secure areas, you should visibly display your badge as well.
- ***Explain to employees*** why accuracy is so important and how high-level functions ensure appropriate oversight.

3. Create a channel for questions and concerns. It's estimated that 40% of fraud is discovered because of an employee tip. But to get those tips, you need the proper channel for questions and concerns. Without such an outlet, employees will head straight to the rumor mill. Establishing pathways for expression – a secure forum, an online equivalent to a suggestion box, or even an anonymous e-mail function – will help employees feel like they're a critical component of the solution, not the target of the system.

4. Foster a healthy culture that leads to high morale. Disgruntled employees – those who feel undervalued, ignored, or overworked – are more likely to commit fraud. Offering plenty of vacation (and making vacation days mandatory), flexible sick leave, and accommodations for personal matters will help employees be on their A-game while also protecting your nonprofit from fraud.

A veteran of Snyder Cohn Accounting (SnyderCohn.com), Steve Braunstein, CPA, was named president in 2010. In addition to his extensive client work, Steve manages and leads the firm's day-to-day operations.

The Right Culture, the Right People, the Right Controls

To create a workplace most likely to deter fraud, see articles such as these at NonprofitWorld.org:

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

Use Background Checks to Avoid Legal Pitfalls (Vol. 29, No. 1)

Vacation Time: More than an Administrative Matter (Vol. 24, No. 2)

Can Your Organization Afford to Lose $100,000? Safeguards Every Nonprofit Needs to Implement (Vol. 30, No. 3)

Protect Your Resources from Insider Theft (Vol. 20, No. 4)

Organizational Culture: It's in the Walk, Not Just the Talk (Vol. 29, No. 6)

Mitigate Cyber Risks with the Right Security Controls (Vol. 36, No 1)

A Path to Stronger Programs, Greater Engagement, *and* Less Burnout? (Vol. 36, No. 1)