Nonprofits Aren't Immune to COMPUTER CRIME

Computers are making crime easier at nonprofit organizations. Here's how to keep it from happening to you.

BY LLOYD DONEY

Computers' ability to transform financial data into speedy, invisible systems has made it easier for criminals to hide their thefts for longer periods. Consider the following:

■ The executive director of the American Parkinson Disease Association admits to embezzling $800,000 over 10 years. This incident occurred not long after it was discovered that the chairman of the United Way looted that charity to fund a playboy lifestyle.[1]

■ The manager of a diocesan pension office is suspected of embezzling over $1.1 million over several years. The perpetrator used some of the money to buy land in Florida and a boat.[2]

■ The ex-treasurer of the national Episcopal Church is convicted of embezzling over $2.2 million. The church recovered all but $100,000, but incurred $321,000 in legal and auditing costs. The perpetrator was sentenced to a 5-year prison term.[3]

■ The treasurer of a youth soccer club is charged with embezzling $46,000 from the club to pay credit card and other bills and to "make ends meet." The perpetrator admitted to taking the money, but claimed he was merely "borrowing" it and planned to pay it back.[4]

■ A priest, working at a private university, confesses to embezzling $100,000 from a program aimed at helping students from low-income families attend college. The perpetrator took the money to fund a drug problem.[5]

■ The chief administrator of the American Cancer Society's Ohio division is accused of embezzling $6.9 million and wiring the funds to an overseas bank account.

■ A former administrator of a local Humane Society is suspected of misappropriating funds, but is not charged due to lack of evidence and the fact that the board acquiesced to her authority by not repudiating her conduct.[6]

■ The resident handyman of a church stole $61,238 from the church over a 10-year period. No one could believe it. The handyman had been a fixture at the church and was known never to have uttered even a mild profanity.[7]

Such cases are all too common. Not only can the loss of money devastate a nonprofit, but the incident can cause a loss of public confidence, leading to reduced contributions.

What Do We Know About Computer Crime?

While there is a sophisticated reporting system for violent crimes, there is nothing comparable for computer crimes (defined as crimes in which perpetrators use a computer as a tool). Although there are few statistics, it is clear that the problem is growing.

The speed and efficiency that benefit the organization serve the criminal equally well.

Studies show that loss from fraud and embezzlement is about 10 times higher when a computer is used than when it isn't. The speed and efficiency that benefit the organization serve the criminal equally well. Further, information housed in computerized systems is invisible. Criminals can conceal data manipulation more easily when review is available only through system access. The combination of speed and invisibility allows perpetrators to steal more over a longer period of time than ever before.

Moreover, many incidents aren't reported for fear of bad press, and many perpetrators are never caught. One investigator was "struck by the incompetence of most of the embezzlers who were discovered. I can't help but wonder what the really clever people are doing."

What Are The Types Of Computer Crimes?

One category of computer crime includes age-old types of crime, such as embezzlement and fraud, with the computer as a new accomplice. A second category introduces a completely new set of crimes unique to the widespread use of computers. This second category includes: (1) unauthorized access, modification, copying, and destruction of software or data; (2) theft of computer time; (3) theft or destruction of hardware; (4) use or conspiracy to use computer resources to commit a felony; and (5) intent to illegally obtain information or property through use of the computer.

Embezzlement is by far the biggest threat to nonprofit organizations. Cash is the most vulnerable asset, since it's the easiest to convert to personal use. Problems that can threaten the very existence of nonprofit organizations typically involve theft of cash in amounts that can be surprisingly large.

Is There A Profile Of The Computer Criminal?

Criminal profiling is a useful tool in investigating and preventing crimes, particularly violent crimes. Unfortunately, profiling is of limited use in computer crime, since the profile of a computer criminal isn't much different from that of the general public.

Computer criminals include men and women of all races and ages, including a grandmother who embezzled almost $500,000 from her employer. In a report covering hundreds of cases over a 10-year period, 75% of perpetrators were men and 25% were women. Most are first-time perpetrators, having no previous criminal record.[8]

However, perpetrators do tend to be relatively young and have better-than-average educational backgrounds. The report includes the following educational information on computer criminals: high school graduate, 42%; college graduate, 45%; and college post graduate work, 13%.

One expert describes computer criminals as "bright, talented, qualified, having good intellects and superior educational backgrounds." Sounds like a perfect employee, doesn't it?

The major threat of computer crime comes not from "hackers" or other outsiders but from your own employees. Yet information on who is committing computer crimes is of little use in nonprofit hiring practices. Virtually anyone qualified for employment is a potential computer criminal.

How Can You Detect Computer Crime?

A sobering reality is that most computer crimes are discovered by chance. Not all nonprofits perform regular audits. Even if they do, audits don't always uncover the criminal activity. An early study of computer crimes[9] lists these ways that computer crimes were detected:

- A bank employee suspected the embezzlement.
- An error was made by the perpetrator when he became too greedy.
- During the yearly audit, auditors detected an inventory shortage.
- A wife reported her husband's suspicious activity.
- An IRS investigation uncovered fraud.
- A police raid revealed gambling activities by an employee, and further investigation turned up massive embezzlement.
- A fellow employee became suspicious.
- A bank messenger failed to deliver checks on time.
- The perpetrator was absent because of illness, and her replacement discovered the criminal activity.

Later data confirm that discovery by chance is still the main means of detection.

How Can You Deter Computer Crime?

Deterring computer crime involves six strategies:

1. Make crime less likely to occur. To do so, focus on these employment practices:

- Conduct background checks before hiring anyone. At a minimum, contact previous employers and perform a criminal-record check. In one case, a bookkeeper, awaiting trial for embezzling

Nonprofit World • Volume 19, Number 2 March/April 2001
Published by the Society for Nonprofit Organizations
6314 Odana Road, Suite 1, Madison, WI 53719 • (608) 274-9777
www.danenet.org/snpo

$773,000, got another job and stole $391,155 from her new employer. In a situation involving a youth counseling center, board members hired an executive director on probation for fraud, evidence tampering, and criminal solicitation. The board discovered the problem only after the executive stole almost $250,000 from the counseling center.

■ Watch disgruntled employees carefully. Don't give them custody of cash, access to accounting records, or authority to approve payments of cash.

■ Train employees that those who steal from their employer will be prosecuted. Studies show that such periodic reminders reduce crime.

2. Make it harder to commit crimes successfully. One of the best deterrents to computer crime is a good system of internal controls:

■ Separate the following functions: bookkeeping, custody of finances, and authority over finances. While this separation is difficult in a small nonprofit, it should be followed whenever possible.

■ Use prenumbered checks.

■ Restrict the number of people who have authority to sign checks.

■ Take advantage of independent safeguards such as bank reconciliations.

■ Supervise employees carefully.

3. Improve detection methods. Perform surprise cash counts and periodic audits.

4. Prosecute and incarcerate perpetrators. Law enforcement officials urge that perpetrators be sent to jail. Although punishing criminals has a limited effect on deterring others, it does keep most computer criminals from repeating their crimes. Data suggest that white-collar criminals, such as those involved in computer crime, have the lowest recidivism rate of all criminals.

5. Use forensic accountants. Forensic accountants have special training and skills that help them uncover criminal activity.

6. Reduce losses. Insure the organization from losses due to employee theft. Bond employees who are in a position to embezzle. Although these measures can be costly, they may be your best protection.

What Is A Nonprofit Leader To Do?

Ultimately, the best solution is an honest employee. But how honest are we? Joseph Wells, founder of the Association of Certified Fraud Examiners (ACFE) estimates that 3 out of 10 people will steal under any circumstances, another 3 will steal under the right conditions, and only 4 in 10 are honest in all situations.

In a *Readers Digest* experiment, wallets containing credit cards and a small amount of cash were dropped. Just over half—80 out of 120 wallets —were returned intact. In a similar experiment, 24 wallets were dropped in Milwaukee with 13 returned.[10] This research suggests that people are a bit more honest than suggested by Wells, but that there is still a disturbingly high level of dishonesty. The director or board member who relies exclusively on trust may be in for trouble.

Most at risk is the one-person office. If the same person must perform the duties of office manager and bookkeeper, some internal controls aren't possible. Even so, there are some procedures every nonprofit, even the smallest, can and should follow:

■ The director should review all bank statements and carefully supervise employees.

■ The board should provide financial oversight.

■ There should be procedures for check signing by the director (or other authorized representative) rather than a check signing machine.

■ Never sign blank checks.

■ Reconcile bank statements regularly.

■ The director or a board member should occasionally do the following: (1) Call some vendors to insure that payments are being made. (2) Call some contributors to insure that contributions have been received, properly recorded, and deposited.

■ Get to know employees. Criminal activity is often accompanied by a change in demeanor or behavior. You may notice, for example, that the bookkeeper seems to be under stress. Such observations are useful in detecting criminal activity. When asked if something is wrong, a perpetrator will sometimes confess.

■ When the crime is committed by the executive director or high-level manager, it is harder to detect, and larger losses typically result. The best strategy for preventing computer crime at the management level is to take great care in the hiring process. Inquire into candidates' backgrounds, using independent sources. In addition, an occasional financial review by an independent party may be money well spent.

■ Report any crime to the proper authorities for charging and conviction.

It's natural to believe your organization is immune from computer

crime because of your worthy mission. The evidence suggests otherwise. If you acknowledge that computer crime can happen and pay attention to what's going on throughout your organization, you're much less likely to become a victim. ■

Footnotes

[1]Stipp, D., "I Stole to Get Even: Yet Another Charity Scam," *Fortune*, 1995, 132(9), 24(1).

[2]Kennedy, R., "Catholic Officials Suspect Longtime Worker in Thefts," *New York Times*, April 10, 1996.

[3]"$2.2 Million Embezzled from Episcopal Church," *Milwaukee Journal Sentinel*, May 2, 1995.

[4]McBride, J., "Man Charged With Stealing From Youth Club," *Milwaukee Journal*, December 8, 1994.

[5]Hermann, P., "$100,000 Discovered Missing From EOP," *Marquette Tribune*, December 4, 1987.

[6]"Former Administrator Won't Face Charges," *Milwaukee Journal Sentinel*, August 16, 1997.

[7]McEldowney, J. E., Barton T. I., and Ray, D. "Look Out For Cletus William," *The CPA Journal*, 1993, 63(44) 44-47.

[8]*Report to the Nation on Occupational Fraud and Abuse*, prepared by the Association of Certified Fraud Examiners (ACFE).

[9]Allen, B., "The Biggest Computer Frauds: Lessons for CPAs," *Journal of Accountancy*, 1977, 143(5).

[10]Kinney, R., "How Honest Are We?," *Reader's Digest*, 1995, 147(884) and Alfvin, C. B., "A Test of Honesty," *Milwaukee Magazine*, 1996, 21(9).

Other References

Barton, T. L., Shenkir, W. G., and McEldowney, J. E. "The Case of Dr. Grayson: Fraud and Abuse at a Not For Profit," *CPA Journal*, 66(2).

Doney, L.D., "The Growing Threat of Computer Crime in Small Businesses," *Business Horizons*, 41(3).

*Goehner, D., "Protecting Your Organization Against Financial Misuse," *Nonprofit World*, Vol. 17, No. 4.

*Messina, F., "Common-Sense Approaches to Fraud Awareness, Prevention, and Detection," *Nonprofit World*, Vol. 15, No. 4.

Smith, J. "Managing Betrayal: A Case Study of Employee Dishonesty," *Association Management*, 49(5).

*Sopher, M., "Setting Up a Control System for Your Organization," *Nonprofit World*,Vol. 16, No. 3.

*Starred references are available from the Society for Nonprofit Organizations, 608-274-9777, Ext. 221, www.danenet.org/snpo.