Edward A. Schirick, C.P.C.U., C.I.C., C.R.M.

Crime Prevention and Risk Management

No Superheroes Need Apply

Does criminal behavior increase during difficult economic times? Some superheroes might say yes and some experts and researchers would agree.

What implications does this have for camps, both for-profit and nonprofit, and small businesses in general? Does this mean camp directors should be more **vigilant** during bad economic times? Is it time to post a job opening online for a superhero? No, wait! Look up in the sky! Here comes "Risk Management" to save the day!

Risk Management is an old friend we can depend upon in good economic times or bad, but only if we are **vigilant**. According to dictionary.com, **vigilant** means "keenly watchful" and "ever awake and alert." If we created a cartoon image of Risk Management, this superhero would have a shirt with a **"V"** for **vigilant** emblazoned on the front, right in the middle. And if we intend to be true to the discipline Risk Management teaches, we will be **vigilant** at all times.

What's the Risk?

The risk of criminal behavior exists in all environments, and although we might wish it to be otherwise, camp is no exception. Unfortunately, the source of criminal behavior is people: our employees, our volunteers, our trustees, and our neighbors, among others. These people are often internal or inside our camp organizations, but they can be external as well. Isn't it ironic that people can be one of camp's greatest assets, and simultaneously one of its greatest challenges and risks?

Employee and Volunteer Worker Theft of Camp Property or Embezzlement of Money

Small businesses — including camps — are most susceptible to employee and volunteer worker theft, because employees and volunteer workers in small business tend to wear many "hats." Small businesses also typically do not have the same kind of controls around inventory, cash, and checks common in larger businesses.

Some of the risks are apparent, but others are new and emerging. Cyber crime is real and growing. Small businesses are more susceptible to cyber crime as well.

Criminal behavior knows no boundaries and all camps are at risk, including closely held family companies, religiously affiliated camps, and nonprofit organizations. . . .

Blessings and Challenges?

Camps operate with a small nucleus of full-time people, or some full-time and part-time employees. Nonprofit operations are supplemented by a dedicated group of volunteer workers, including board members and trustees.

Small groups of dedicated people are both a blessing and a challenge. While we might wish for the blessings to last forever, the truth is circumstances change and what was once a blessing can become a problem.

When people commit "white collar" crimes, we sometimes read stories about the matter in the newspaper. The stories have common threads and are often about a dedicated and trusted employee who embezzled thousands of dollars. The reasons vary. One story said the motivation was to pay an ailing spouse's medical bills. Another tells about the patience of an accounts payable clerk who systematically siphoned off thousands of dollars paid annually to a fictitious vendor she established. The reason was that she was living beyond her means, a lifestyle unknown to her fellow workers and not evident in her clothing or demeanor at work.

When we learn of these stories we are often surprised, but stories about employee theft don't always make the news. Sometimes these stories don't surface at all, because the owners (the victims) are embarrassed, or because the amount of money involved was relatively small, or they didn't want to prosecute the formerly trusted employee for their own personal reasons.

Prevention and Reduction — Be Vigilant

Because circumstances do change and not all employee white collar criminal behavior is reported and prosecuted, owners and directors must take steps to protect the assets of their camp and reduce the exposure to employee theft.

There are some fundamental practices all businesses should be following to reduce the risk of employee theft around money. These include procedures to protect cash, checking accounts, checks received from customers, checks being sent to vendors, payroll checks, and credit card receipts.

Every business is different to one degree or another, but taking steps such as the ones that follow may be helpful:

- Keep petty cash in a safe, or secure it in a locked cabinet.
- Separate check writing duties from checking account reconciliation duties.

continued on page 23

Risk Management continued from page 20

- Put blank checks in a safe or locked cabinet.
- Consider a periodic, unannounced audit of accounts payable.
- Establish a dual signature requirement for accounts payable checks above a certain dollar amount.
- Establish spending limits on credit cards used by employees.

Develop your set of practices and procedures to reduce the risk of employee theft, and then consult with your accountant for refinement of your plan or for other ideas.

One practice to reduce the risk of employee theft of equipment and business property is to establish an inventory by department. Assign someone outside of the department the responsibility to keep it current. Check it regularly.

Other Practices

It is recommended that all prospective employees and volunteer workers, not just seasonal counseling staff, complete an employment application. This includes prospective board members and trustees, too. The application should include questions about whether the applicant for your position has ever been convicted of a crime.

Prospective employees, volunteer workers, board members, and trustees should also be willing to authorize a criminal background check. Unwillingness to do so should stop your process.

Also consider asking all employees, volunteer workers, board members, and trustees with responsibility for handling money (including pension funds) to consent to a credit check in addition to the criminal background check.

Vigilance encourages policies requiring all employees (full-time, part-time, and seasonal), volunteer workers, and board members, regardless of their tenure, to undergo a criminal background and credit check every five years or so, especially if volunteer workers, trustees, or directors have access to money in accounts or check-signing authority.

Seek information from advisors — accountants, lawyers, insurance brokers, and risk managers — and increase your awareness about risks and controls being used by other businesses to prevent white collar crime.

Disgruntled Employees

Some employees leave when they become disgruntled and unhappy. Others may stay on and conspire with people inside or outside your organization. In some ways, technology has made it easier for employees to commit crimes.

For example, does your camp management database contain Social Security numbers of customers? How about credit card numbers? Would it be possible for an unhappy employee intent on stealing to access the database and sell the information to someone who might then steal your customers' identities?

What is your policy about allowing notebook computers or flash drives with customer information out of the office? Does your camp management database allow you to restrict employee access to certain personal information about customers such as Social Security numbers and credit card numbers?

Other disgruntled behavior may involve sabotage or destruction of databases or software, acts of vandalism designed to deprive you of the use of your property and cost you money. Other employee risks involve facilitating an attack against your computer network by downloading inappropriate software or e-mail to his or her computer.

The risks associated with cyber crime are changing constantly. Seek information from camp management system administrators to determine what safeguards they have programmed to reduce these risks in your camp.

Legal Compliance Issues

The Employee Retirement Income Security Act of 1974 (ERISA) requires that trustees of pension plans such as 401(k) and 403(b) be insured against dishonest actions in their roles as trustees. The limit requirement varies from year to year and is equal to 10 percent of the net asset value of the pension plan assets as of the end of the calendar year.

The risk management process will serve you best when you stay focused on constant improvement.

Failure to comply could put the organization at risk in addition to the individual trustees who are individually and jointly responsible under this law.

If you are uncertain about compliance with ERISA, contact your insurance broker or accountant to review this matter further.

Other Crime Risks

Besides white collar crimes involving employees, there are other risks which should be considered as part of a comprehensive risk management crime prevention program. Consider the following:

- Theft of money or property by others — not employees
- Theft of camper money or property
- Vandalism
- Arson
- Sexual abuse and molestation
- Assault and battery/bullying
- Abuse of alcohol and drugs

Be Vigilant

Remember to stay in touch with your superhero, Risk Management. The risk management process will serve you best when you stay focused on constant improvement. Be ever awake and alert. Try to avoid complacency and the thinking that suggests: "It can't happen to me."

After you have determined you've done your best to reduce the risk of white collar crime, buy an appropriate amount of crime insurance to protect your organization, just in case. Because even though crime risk can be managed and prevented, it can never be eliminated entirely.

Edward A. Schirick, C.P.C.U., C.I.C., C.R.M., *is president of Schirick and Associates Insurance Brokers in Rock Hill, New York, where he specializes in providing risk management advice and in arranging insurance coverage for camps. Schirick is a chartered property casualty underwriter and a certified insurance counselor. He can be reached at 845-794-3113.*