

Keeping Watch

by Lisa M. Starr

In a business where narrow profit margins are more common than not, every dollar counts.

Unfortunately, as the spa industry grows in numbers of locations, employees and clients, so do the opportunities for losses stemming from theft and fraud. The 2003 National Retail Security Survey conducted by the University of Florida in Gainesville, Florida, estimates that retail businesses in 2003 experienced shrinkage losses of approximately 1.5%. This may not sound like a lot, but it represents more than \$32 billion dollars! Of that total, 47% was attributed to employee theft, 32% to shoplifting, 15% to administrative error and 6% to vendor fraud. These numbers clearly reflect the need for such businesses—including day spa businesses—to develop a loss protection plan.



Employee theft is a well-established problem; every spa owner must take steps to prevent such losses.

Your loss protection plan should start with your employment process.

According to Joe “Mac” McConnell, director of small business sales and marketing for ADT Security Services, the top five loss prevention concerns of small business owners nationwide are, in order:

1. Burglary/intrusion detection
2. Shoplifting
3. Liability (such as on-site arrests, drugs, violence or harassment in the workplace)
4. Employee theft
5. Intellectual property

To develop a loss protection plan for your business, your first step should be to perform a “security audit.” This involves sitting down with your management team and looking at your business from an outsider’s perspective. You’ll want to focus on three areas: identifying your company’s valuable property and assets; evaluating possible risks; and determining priorities for action, using the above list of five potential risk areas as a guideline.

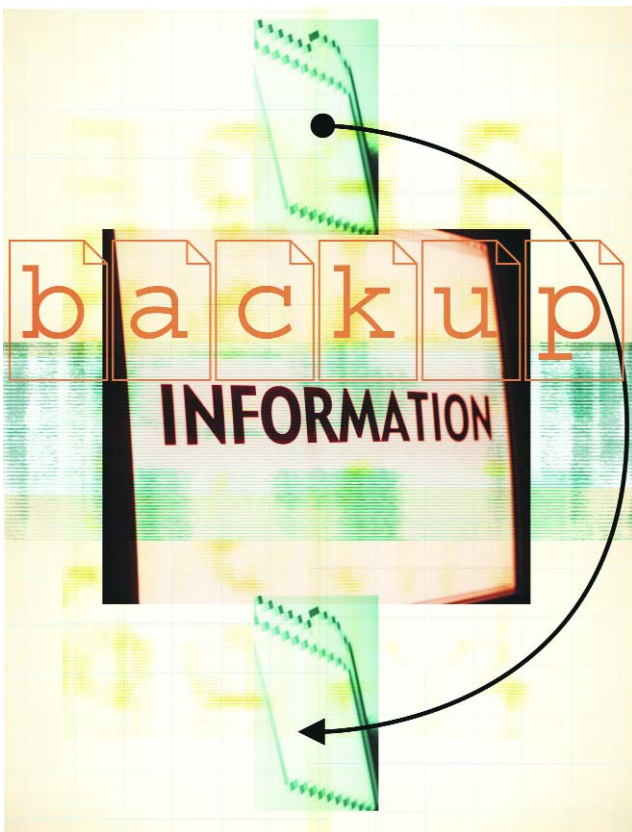
Step two is to develop an action plan to correct any deficiencies or improve operations. According to the Department of Commerce, 30% of all business failures are caused by employee dishonesty. This fact highlights the need for management to establish and implement policies and procedures that help employees understand their role in the prevention of losses.

Plugging the Leaks

Internal security. Your loss protection action plan should start with your employment process. Do you perform background checks on prospective employees? In the National Retail Security Survey, over 70% of the businesses involved conducted multiple interviews, verified past employment, and performed both criminal background and personal reference checks. This oft-neglected area is a good place to start minimizing your risk. A structured orientation program for new hires, in which you discuss the company’s mission, values and procedures, is another useful tool.

Next, establish certain operational procedures, especially for the front desk. “In order of priority, you’re looking to secure employees, customers, cash and merchandise,” says McConnell. “Start with the basics, such as defining the earliest and latest times for opening and closing; policies for the handling of cash, bank deposits and drops; and having supervisors verify large cash or check transactions. For employee safety, your policy should dictate that at least two people close at night, and walk out together.”

Information storage. Another frequently overlooked area in spas is the technology arena. Since computers and software are relative newcomers to our businesses, we haven’t all come up with



Your computer system needs a simple backup system that managers can use daily to limit access to sensitive data.

It's common
to keep a
business
week's worth
of digital
tapes.

proper procedures for managing and securing both computer equipment and valuable data. The more you depend on these data to run your business, the higher the priority you need to place on securing them.

Your computer server should be kept in a protected area of your spa, such as a mechanical closet or storage area adjacent to the management office. The server should not be under the front desk, where the risks include accidentally turning the server off, overexposure to dust and dirt, and deliberate sabotage. The server, and any routers or hubs to your computer network, should be kept secure, along with your telephone system.

To protect your data, backups need to be performed every day

your spa is open for business. Your server should be equipped with a digital tape drive and the software necessary to make copies of your data. The backup is typically scheduled for the early-morning hours, such as 2 a.m., when there's no chance that anyone would be on the system. It's common to keep a business week's worth of digital tapes, each labeled with the day of the week, so that if something were to go wrong you would have more than one backup. To be completely protected in this area, make sure a backup copy of data is kept off the premises, and that you know how to restore your data from the tape should you ever need to.

It's also necessary to use passwords with your computer system. Spa service providers typically only need to see their own clients' information and overall appointments for the day. Your front desk staff would obviously need to be able to get into the point-of-sale

section of the program. You may want to protect functions such as running and printing reports, modifying or voiding transactions, issuing gift cards or gift certificates and closing the register.

To protect all of your hardware, be sure to keep a log of the serial numbers of any pieces of computer hardware, including the computer itself, monitors, credit card machines, hubs or routers, and printers and fax machines in a locked safe. You might even etch your postal code and company name and/or logo into the casings of the equipment in a prominent location.

Intellectual property. During your risk evaluation, you may identify among your assets some valuable documents unique to your spa business. You may have invested a great deal of time into developing your employee handbook, department training manuals, service protocols and operations manuals. These materials, along with employee and client files, are full of proprietary information and, as such, should be protected. They should not be available digitally, and your employee handbook should identify these and any other documents you have developed as confidential and clearly the sole property of the business.

Inventory control. In the spa industry, most of the inventory that we manage consists of the professional products we

Security Web Sites

- Adt.com
- Americanexpress.com/open
- Securityworld.com
- Microsoft.com/smallbusiness
- Nrf.com (National Retail Federation)
- Asisonline.org (American Society for Industrial Security)



Modern security systems often include keypads, which allow employees to enter without keys and owners to immediately block the entry of ex-employees.

use in our treatments and the product items we retail. Providing purchase orders for items that are used regularly can ensure that those items are the only ones ordered from your vendors. Using the inventory portion of your software to establish minimum and maximum supply levels and create purchase orders provides a great level of control, especially for retail items. You also need procedures for receiving, unpacking, storing and displaying professional and retail merchandise to minimize waste and the opportunity for losses due to mismanagement.

Access management. Preventing burglary is the No. 1 security concern of most small business owners, and the best way to do this is with some form of intrusion detection. Irwin Dunsky, owner of C.A.T. Alarm Systems in Matawan, New Jersey, recommends a simple burglar alarm system, protecting the perimeter doors with motion detection. (Dunsky notes that most thieves won't bother with breaking a window to gain entry, so he doesn't recommend window alarms unless your spa is in a high-risk urban environment.) When activated, the alarm sends a mes-

sage to a central monitoring location where personnel will call the police and the facility directly. Modern systems can come with a keypad at the door, enabling employees to use individual codes to gain access, rather than a key. Dunsky estimates that a system for a 2,000- to 3,000-square-foot facility with two or three doors would cost approximately \$1,000, with a monthly monitoring fee of between \$25 and \$35.

Newer systems have key-card controls, which can allow you to limit access to specific areas, such as storage rooms or offices. These systems typically cost about \$7,000 to \$8,000 (including installation) for a facility with three doors.

A great advantage to both the keypad and key-card systems is that they eliminate the need to rekey locks when an employee leaves the company; he or she is simply removed from the system.

Some security service companies can also provide you with a monthly report of all access activity, letting you know when your doors are being opened and by whom. This is particularly useful for owners and managers



Digital Video Recorders make security cameras cheaper and easier to use.

who are not always on the premises. This reporting feature adds about \$1 per day to the price of the system.

New technology. Many business owners feel most secure and in control by utilizing a closed-circuit television system. The big technological advance here has been the advent of DVRs, or Digital Video Recorders, instead of video tape on a loop. Since DVRs entered the marketplace, they've quickly become the preferred option because of their greater reliability, storage capability and convenience. With a DVR you can search through any archived information much more quickly and easily than you can with a VCR tape. You might choose to place one camera for your front desk area or, in a larger facility, more cameras for areas like your back entrance, employee break room and inventory storage areas.

Spa director Justin DePasquale of DePasquale Salon & Spa in Morris Plains, New Jersey, uses a DVR system to monitor the facility, which spans 24,000 square feet, has 190 employees and eight separate entry doors. The system has 16 cameras and a main control center in the spa director's office. "We added this system because we were getting so large and wanted to feel more in control, especially of our access," says DePasquale.

"Having this system doesn't save us any money—we still need the proper amount of personnel to run the organization—but it does give us peace of mind. We have a lot of female employees who may be leaving late at night, and we want them to feel protected. The system helps everything run more smoothly and makes everyone feel safer." Some of the cameras in DePasquale's system are trained on waiting and reception areas, to allow the office staff to see when things are getting backed up and respond with additional personnel.

Security Tips

- Maintain a neat, attractive and well-maintained business setting, a sign of effective management.
- Make sure that your facility is well lit, especially at night.
- Minimize the amount of available cash on site.
- Train employees to make eye contact with everyone who enters your establishment.
- Conduct background checks on prospective employees.
- Establish policies and procedures for sales and cash control.
- Have a written policy and procedures manual.
- Keep detailed records of inventory.
- Make sure you understand your books. If you're not a "numbers person," spend some time getting familiar with your business' systems for record keeping.
- Keep your accounting software on a separate computer.
- When possible, use online account management and bill payment.

“Can you put a dollar value on avoiding a robbery?”

A system of this considerable size and capability costs around \$30,000, but there are lots of other options in DVR systems. “The number of cameras and size of the recorder are determined by your needs for memory and playback time; therefore, the price of the system will fluctuate greatly,” says Dunsky of C.A.T. He adds that another great advantage of the digital system is that if you have high-speed Internet access, you can hook up the system and watch it remotely, either through your network or its own network.

A final question on DVR systems concerns whether to record in color or black and white. According to Dunsky, color systems—which once cost twice as much as black-and-white systems—now only run about 10% more. McConnell of ADT advises, “If you’re trying to identify someone you don’t know, you would prefer to have color. If you’re just monitoring employees in your facility, you could probably go with black and white.” For example, color would certainly be more useful if you were using your system to identify shoplifters and needed clear, specific descriptions.

An Ounce of Prevention

Obviously, the needs of every business are different. But in an econom-

ic climate where half of all new businesses fail in their first two years, establishing loss prevention guidelines is a worthwhile enterprise. McConnell advises retail business owners to allot about 1/2% of their gross revenues to loss prevention programs, all the while evaluating the risk of loss versus the required investment. “Deciding what to spend is all relevant to what your problem is,” he notes. “Can you put a dollar value on avoiding a robbery? What are you losing annually? And how can you identify how much to spend in order to keep from having a problem?”

The goal of using a security system is not to catch someone in the act of stealing but to prevent the theft from happening in the first place. Such prevention starts with the ethics and values of the company and its management. The hardware is just icing on the cake; your primary strategy should be to establish a program for loss prevention and train all of your staff members to work together to ensure a secure and successful environment. ♦

Lisa M. Starr, a spa and salon business consultant for Lipsync consulting and Preston Wynne Success Systems, is based in the Philadelphia metro area. She can be reached at lisastarr@aol.com.