

# Security Director's Report December 2002

## Should You Ever Bend the Rules of Your Ironclad Security Policy?

While SDR has never advocated shying away from investigating workplace crime to avoid stepping on a few toes, the thorny world of workplace litigation makes cost/benefit concerns a factor in how-or how aggressively-security departments should respond to different events. Our advice? To effectively investigate in this current murky environment, security departments need to strike a balance between concrete procedures from which they never sway and flexibility. In short: There are times when security needs to "say one thing while doing another."

Case in point. Your security policy calls for a written incident report in every case that the security department investigates. Generally speaking, that's smart. But should this rule be ironclad? Maybe not, suggests a real-life cautionary tale from the case files of the Lubrinco Group (New York City; 212-695-1759 ; [www.lubrinco.com](http://www.lubrinco.com)).

Scenario: Having spent the afternoon drinking at a bar at a Dallas resort, a married woman and her boyfriend get the urge to slide down the property's banister on their way out. The woman falls off, breaks some clay pots, and heads back to her room with minor injuries. Security calls and insists they need to speak to the woman, but the guests say they are unhurt and hang up. Security then knocks on the couple's door, again insisting they speak with the woman in order to fill out their incident report. Fearing news of their affair will somehow leak out, the guests ask security to leave and not to file a report. When security refuses and remains outside the door, the patrons escape out a window, pulling down a drain spout in the process.

When the woman later calls the hotel to speak with her sister who is another guest, security personnel, now more anxious to settle the matter because the damage has become more costly, break into her phone conversation. Rebuffed again, security turns the matter over to the police who call the woman at work the next day and notify her they've taken a formal report from the hotel for the criminal damage she and her boyfriend allegedly caused.

The result? You guessed it: After involving the police, attorneys come next. Before long, the hotel is facing a lawsuit for negligently serving too much liquor, having an "attractive nuisance" (the banister), failing to take safety precautions in the event someone were to slide off the banister, and breach of privacy for cutting into the phone call. The hotel ended up settling out of court for roughly \$ 400,000.

Was the hotel entirely in the wrong? No, say the investigative experts at Lubrinco. Should they have handled the incident differently? "Clearly yes. The hotel should have sent a concierge or assistant manager to inquire if there was anything he or she could do to help and to inquire about what to do regarding the damage caused to the plants." According to the plaintiff, she would have gladly paid on the spot out of pocket to avoid a report. Instead, she wound up pocketing \$ 400,000 of the hotel's money.

Workplace searches. This is another critical area where security departments may want to have one thing on the books, but occasionally follow a different policy in practice, suggests Jonathan A. Segal, Esq., a partner in Wolf Block Schorr and Solis-Cohen LLP (Philadelphia; 215-977-2000; [www.wolfblock.com](http://www.wolfblock.com)) in HR Magazine (Society for Human Resource Management, Feb. 2002).

Segal notes that some companies—in an effort to appease employees—write a security policy that limits their right to conduct searches to cases where there is "reasonable cause." This is a bad idea, he says, because it can restrict you legally, and in an emergency you may not have the luxury of only searching individuals' work areas where you have reason to believe you'll find weapons or explosives.

It's better to offer no qualifiers. Don't restrict yourself by saying you will only search with "reasonable cause," and don't make a point of saying you have the right to search "randomly"—this will unnecessarily agitate some workers. In your security policy, simply reserve the right to search the workplace. (Note: Define "workplace" as broadly as possible. This comprises employees and their belongings when on the premises, employees' cars on the premises, surrounding grounds, owned and leased facilities, and so on.)

However, as Segal notes, just because you possess the right to search—and reserve that right via your policy—does not mean you can afford to avoid doing a serious risk/benefit analysis each time you want to conduct a search. Searches often come with consequences, he notes. Other experts agree that, because of the highly intrusive nature of a search, individuals who are subjected to them often jump on the chance to bring a lawsuit:

Searching an individual of a protected group may lead to costly discrimination claims. Solution: Search only when you have a legitimate, business-related, and well-documented reason to do so.

Searches can turn up medical or other critical personal information, the exposure of which an individual can use as the basis for a lawsuit. Solution: If employees indicate that they have confidential items in their briefcases, desks, etc., offer them the option of having the object or area searched by a third party, advises Segal.

Employees may refuse to cooperate with the search, which can lead to a physical confrontation that results in a civil harassment claim. Solution: Always have a witness present who can testify to what was and wasn't done during a search.

Searching female employees may lead to a sexual harassment or sexual assault claim. Solution: Have a person of the same sex search the employee.

If the subject of the search is a bargaining unit employee, trouble with the union may be on tap. Solution: Have a union shop steward present at the search, advises Segal.

While fear of a lawsuit shouldn't halt security department investigations, it should compel you to delay them until you're sure they're worth the risk. Only search when (1) you believe you will find what you're looking for, and (2) what you're looking for is worth the risk that accompanies the search.

Polygraphs. Companies will pay dearly for any missteps if they go this route during a workplace investigation. Nonetheless, roughly 5% of companies administer lie detector tests to employees annually, according to annual privacy surveys by the Society for Human Resource Management (SHRM; Alexandria, Va.; 703-548-3440; [www.shrm.org](http://www.shrm.org)). The Employee Polygraph Protection Act (EPPA) limits when you can give an employee a polygraph and has strict standards for how you have to conduct such a test. (For easy-to-understand answers about the EPPA, see "Q&A: What You Need to Know About Lie Detector Testing," SDR July 1999.)

You should also know that, as risky as polygraphs have always been, a first-of-its-kind federal appeals court decision in May suggests they're getting a little riskier. (*Calbillo v. Cavender Oldsmobile, Inc.*, U.S. Court of Appeals for the 5th Circuit.) The court ruled that a private investigator, who recommended

and then administered a polygraph test to a suspected employee thief, is not an "employer" under the law, and so it dismissed the employee's lawsuit against the firm.

What's the significance? For companies and their security departments, it indicates a further unwillingness of courts to hold the investigators who give lie detector tests liable for them. While employees can try to sue the investigators who administer the tests, they are far more likely to successfully sue their employers. This case doesn't put companies in any more danger so long as they follow the letter of the EPPA law, but it does suggest that if missteps occur, you may not be able to point the finger at anyone else.

In fact, while the courts rebuffed the employee's claim against the investigator in this recent court case, the employee successfully settled his lawsuit against his employer. While the amount is sealed, it's safe to assume that the car dealer lost more because of its investigation than it had from the stolen freon that sparked the investigation in the first place.

Video surveillance. This is one investigative area where inflexible security department procedures may be smart, regardless of how serious the crime is that you're investigating. Consider this case profiled at the National Employment Law Institute's (NELI) Employment Law Briefing, in Vail, Colo., in March. A Maryland hospital, plagued with disappearing narcotics, placed a video camera in the nurses' locker room. Compelling business interest? Sure, but still an invasion of privacy, a judge subsequently ruled.

What should be your guide? Here is an answer from NELI presenters and employment law specialists John Fox and Enrico Alis, with the law firm Fenwick & West LLP (Palo Alto, Calif.; 650-494-0600; [www.fenwick.com](http://www.fenwick.com)). To avoid state constitutional claims for invasion of privacy:

Establish a written policy notifying employees in advance that video surveillance may take place, and require employees to sign a document stating that they received notice of this policy.

Document the need for surveillance in the case you are investigating.

Never set up video surveillance equipment in areas where employees may have reasonable expectations of privacy. You will almost always find it impossible to justify use of video surveillance in private areas of the workplace, such as locker rooms and rest rooms.

Follow the above guidelines and common law invasion of privacy actions by employees won't get off the ground, suggested Fox and Alis.

For more information: SHRM (Alexandria, Va.; 703-548-3440; [www.shrm.org](http://www.shrm.org)) is a good source for additional information on workplace privacy, the law, and workplace investigations. The NELI presentation, "Privacy Inside and Outside the Workplace," is now available on the Web ([www.fenwick.com/About\\_Fenwick/National\\_Employment\\_Law\\_Institute.com](http://www.fenwick.com/About_Fenwick/National_Employment_Law_Institute.com)).

Copyright © 2002 IOMA