A Warm Welcome to All Who Enter Our Facility. . .Maybe Not

By Joel Hershkowitz, Idesco Corporation

Being a conscientious plant manager or supervisor, you have taken steps to insure your plant is safe and secure for the employees who work for you. Today, there isn't a facility around that hasn't taken steps to protect it from intruders. Just about everyone carries an identification card from his or her place of work. Access control systems are in place and many buildings are fenced in, some with barbed wire for added protection, many if not all with 24-hour guards and a main gate entrance. Yet, with all of that security in place, there still is the possibility of having many "intruders" entering your facility on any particular day and at any given time. In may not come immediately to mind to consider a "visitor" to your building an intruder, but who is the person you've just let in, anyway? He's not an intruder; he's been here just about every day for some time now. Or we use his service every week. Or he's just here to see a friend.

Say you have decided to expand your facility, or upgrade some plumbing or electrical work. Most likely this is going to require the work of an outside contractor (or two). So you hire two firms, which of course are "reputable," and they begin their work. But do you know any of the employees who are working for these contractors? You have done extensive checking of your own employees, and their access to your facility may be limited to their job function, i.e., engineering or accounting. Now suddenly you have people who have not been directly hired by your staff who may have access to several areas. They are to a certain extent "a security risk" to the company. Sound far-fetched?

The original *Mission: Impossible* series of the 1960s had many plots where a contractor of one kind or another was actually one of them. They were disguised as delivery men, firemen, repairmen and so on. Their uniforms were their "ID" and they were not questioned as they gained virtually complete access (to the facility) and went about their business.

Just what damage can a not so well-meaning visitor cause?

- Espionage-When left alone, gaining access to the facility serves as an easy way to observe, listen, take pictures, record and take notes.

- Data Theft-Along the same lines, data theft can give other companies or other countries all the information they need to catch up or even pass you competitively.

- Sabotage-Unattended, a visitor can start a fire, place an explosive, jam up equipment, change equipment settings, emit poison gases into the air.

- Revenge-Those who feel you have done them wrong can have someone get in and do all of the above to get even. In a school environment a visitor may be an ex-boyfriend or girlfriend, or a relative out of favor whose goal is to take a student out of school against a parent's will.

- Material Theft-Unattended, a visitor can steal valuable equipment, manuals, personal items, money.

- Accidents-Visitors may have good intentions in their visit, but if left unattended, they may fall victim to an accident by entering the wrong place or by not following instructions. In the case of an emergency, visitors can be a real liability.

Outside contractors--those hired for a period of time for construction, repairs, etc.--are visitors who are going to return again and again until their job is complete. While they may not be paid for their work by your company, they will in many cases have to follow the same safety and security rules that have been set up for your employees. In some cases it may be just common sense, in others it may be because of the law. Take contractors who are working on electrical equipment. They are going to have to follow the OSHA Standard 1910.147: The control of hazardous energy (lockout:tagout), just as your employees must. The contractors' lockout:tagout procedures may be slightly different from yours as their equipment may be functionally different, but they will be following the overall lockout:tagout rules.

And according to 1910.147(f)(2)(i): Whenever outside servicing personnel are to be engaged in activities covered by the scope and application of this standard, the on-site employer and the outside employer shall inform each other of their respective lockout or tagout procedures.

Recognizing that *outside contractors' overall procedures may be different from those created for the permanent employees at the facility,* OSHA states in 1910.147(f)(2)(ii):

The on-site employer shall ensure that his/her employees understand and comply with the restrictions and prohibitions of the outside employer's energy control program.

Another important note with regard to overall lockout:tagout training, 1910.147(c)(7): *The employer shall provide training to ensure that the purpose and function of the energy control program are understood by employees and that the knowledge and skills required for the safe operation, usage and removal of the energy controls are acquired by employees.* It is extremely important that both the permanent employees and outside contractors have a working knowledge of each other's lockout:tagout procedures, even if they are obliged to follow only their own.

A potentially dangerous group of visitors to your facility can be a contracting unit called in to help deal with hazardous chemical operations. According to OSHA 1910.120(b)(1)(ii): An employer who retains contractor or subcontractor services for work in hazardous waste operations shall inform those contractors, subcontractors, or their representatives of the site emergency response procedures and any potential fire, explosion, health, safety or other hazards of the hazardous waste operation that have been identified by the employer's information program. *Outside contractors in this situation have to quickly learn your firm's process safety information, to include flow diagrams, piping and instrumentation diagrams as well*

as detailed narrative descriptions of the methodology required.

Training or refresher training may be required of these temporary employees. And certification of knowledge and skills may be required. All this is from a safety point of view. From a security view, with these "outside" employees working on such critical areas within your facility, you are counting on the background checks handled by the outside contracting firm(s) that have been hired. In a post 911 era, you and your contractor must know as much as the law allows about the people coming to work in your facility.

Then there are the general service groups that stop by your facility periodically. Take the monthly exterminator visit, for example. We don't generally give much thought to the friendly gentleman who is protecting your facility against mice and roaches. But is he hurting as much as he is helping? Many pesticides used today can cause or contribute to both nervous system and respiratory disorders. So it may not be unusual for an inordinate number of employees to be calling in sick after a pesticide treatment and your company management just scratching their heads trying to understand why. Bottom line: *Be conscious of whatever type of contractor you use for everyday maintenance and upkeep at your facility. Along with knowing their advantages (in this case, no mice or roaches), make sure you know the disadvantages, including those that are health related.*

The evening and weekend cleaning service have worked for you for years. A not too careful mixture of the ammonia they use can cause your employees to wind up with eye and throat irritation. Furthermore, the laundry and cleaning products used may result in a sudden release of chlorine if incompatible products are mixed, leading to respiratory exposure for all.

You may have taken your time or not concerned yourself too much about dealing with OSHA regulations pertaining to handicap accessibility. That is because you simply do not have any handicapped workers. But the law doesn't only apply to employees. It also applies to visitors. And, the Commerce Department's Census Bureau data released in March of 2001 states that some 53 million people have at least some level of disability. 29CFR2205. 150 deals with the Enforcement of Nondiscrimination on the Basis of Handicap

in Programs or Activities Conducted by the OSHA Review Commission Concerning the Program Accessibility for Existing Buildings. According to 2205.150(b)(1): General: The agency (facility) may comply with the requirements of this section through such means as redesign of equipment, reassignment of services to accessible buildings.... The agency is not required to make structural changes in existing facilities where other methods are effective in achieving compliance....

Then there is the everyday visitor to your facility. He or she is there for a business meeting, to make a sales presentation, look through your showroom, do an audit; take a tour; attend a seminar, or do volunteer work. Some facilities may have hundreds of visitors a day. To handle so many people and maintain control of them, many companies have decided to "ID" these visitors in a manner similar to the way they do their own employees. Now, to "ID" your own employees can involve a fairly large expense and the management of an extensive database.

That isn't quite necessary when handling visitors who may be in the facility for a day or two or three. And so many security companies have developed software programs and equipment that can produce a visitor ID badge that is relatively inexpensive.

Many of the programs make it easy to produce a badge by first scanning the person's business card or driver's license, saving the information in a database, taking a digital photo, then printing onto a pressure-sensitive label for easy application of the badge onto a piece of clothing. Once the registration is complete, an e-mail can be send to the person and department expecting the visitor to both announce and confirm the receiving of the visitor. Some programs provide a barcode, which makes it easy to track visitors as they move about the facility and/or insures that they arrive at their planned destination. It is also used to insure that they have checked out at the end of the day, or by whenever the expiration of the planned visit is scheduled.

When large numbers of visitors are expected from a particular group, say, for a seminar, they can be pre-registered. The group sponsoring the visit can send all the information that is required by your facility to have someone registered via e-mail.

When the group arrives, a check of their driver's licenses will allow the op-

erator of the visitor system to call up those names from the database and quickly print out badges.

That is all well and good, but while it has become easy to quickly get your visitors accounted for, what about people you DON'T want in your facility? Perhaps there are employees who have been terminated for one reason or another. Or, an employee has a relative (perhaps an ex-husband or boyfriend she no longer wants to see. Or, perhaps your facility is a school and you have been given specific instructions as to who can and who can't pick up a child at the end of classes. You will find that there is visitor software that provides a "Watch" list. That list contains names of those who are not allowed in (for whatever reason). It may also contain a picture or pictures of the person, as well as specific instructions as to what should be done should one of them make an appearance. For example, on a name and picture match, the message that may appear could be "CALL POLICE IMMEDIATELY." *Visitor software is constantly monitoring the total number of visitors within the facility at one time, as well as the total number of visitors in a particular area or visiting a particular person.* Hospitals use this feature to monitor how many visitors are visiting a patient. This allows the hospital to keep control of the situation, based on their visitor policy, and order a patient's condition.

Another advantage of visitor software is the ability for any member of your staff to design a badge with little training. So, if you have a number of different groups visiting the facility, a different badge can be designed for each group in just a few minutes. With a different badge design for each group, it becomes easy to track and stay in control of their movements. "Self-expiring" labels can also be placed onto the printed badge as a way of determining if the visitors' allowed time in the facility has lapsed. They are available in half-day, whole-day, one-week and one-month increments. Once placed on a badge and activated, the expired message will show through the Visitor message at the appropriate time. Most of the available software contains Report Generating Capabilities. So, at the end of a particular time period (perhaps at the end of the day), a report can be produced which can clearly show check-in, check-out times of all visitors-and who has remained in the building-both authorized and unauthorized.

Besides security concerns, these reports are also important in the event of an evacuation, lockdown, or other type of emergency situation.

Some of the more sophisticated software packages allow for seamless integration with a company's access control system. A temporary badge will have the ability to automatically control turnstiles, doors, portals-all electronic entry points during one's allotted time and allowed visiting area.

One of the most dangerous visitors to enter a facility isn't a human being. It isn't alive for that matter. It's your mail. Most visitor software packages also allow for the tracking of mail from entry point through delivery to its intended receiver. Barcode symbology is used to manage fields to include the shipper, a tracking number, intended employee name and the date and time the package was delivered.

While all of the available software packages are easy to learn, the real training is in the discipline involved in following the procedures for every single visitor.

When visiting a highly secure area, such as a government building (a research center, for example, you can expect security to be even tighter. Before a visitor heads for the secure facility, the host or sponsor of the trip will have had to submit that person's name on the next day's visitor list. And that would have had to be done by a specific time, probably early in the afternoon of that preceding day. Upon arriving at the gate of the secure facility, at least one form of ID will be required with at least one form containing photo identification. Signature verification may also be required. After verification, a Temporary Entry Pass is issued. That pass will allow travel from the initial entry point only to a Security Operations (Visitors) Center, which is completely separate from the rest of

the facility. If the visitor's vehicle is allowed to proceed to the center, it will surely be searched. If it is not allowed to proceed, it will be left in a guarded area and a shuttle bus will be provided. Once at the center, the visitor name will be checked against the day's manifest. Only those on the list will be allowed to proceed. If the person's name is not on the list, the host or sponsor will have to

---

**VISITORS' SAFETY AND
SECURITY CODE OF CONDUCT**

The following is for the benefit of everyone involved in the operation of a facility.

- Anyone who is not an employee or administrator of a facility will be considered a Visitor.

- All Visitors must be registered and issued an identification badge.

- Visitors should only be issued a badge after displaying a valid ID.

- Visitors shall not be permitted on the grounds during when the facility is closed without the express authorization of the highest level in the management chain of command.

- All Visitors will follow all safety and fire regulations and evacuation procedures (clearly) posted. This information should be posted in English and at least one other language, depending on the geographical location of the facility.

- Visitors are not permitted to have in their possession or use any controlled substance, illegal drug or alcohol while in the facility.

- Smoking may be prohibited at the request of the employees or by the nature of the work being performed at the facility.

- Visitors shall not interfere with the work of employees or any other type of operations taking place in the facility.

- Visitors shall not engage in harassment, including but not limited to sexual harassment of either employees of the facility or to other visitors.

- Visitors shall not be in possession of fireworks, weapons, ammunition, explosives or incendiary devices while in the facility.

- Visitors shall not be in the facility with the intent of inciting others.

- Visitors shall not misuse computer equipment by attempting to tamper with hardware, software, disks, files or passwords.

- Former employees of the facility who return for a (casual) visit shall be considered Visitors and are subject to the Visitors' code of conduct.

- Special procedures and actions will be put into place to accommodate Visitors.

---

verify the visit with security. Visitors can also be expected to pass through a metal detector, have their bags, backpacks and purses X-rayed, and be subject to a physical search. When a person is cleared by security personnel and verified as an official visitor, he or she will be issued a proximity card tailored to provide access only to those areas absolutely required for the visit and a visitor ID card. (It is possible that the two can be combined on one card.) Even with the proximity card in the visitor's possession, an escort may be assigned to control movements to the proper location.

Delivery personnel to these secure areas, who are of course visitors by their own right, must have a bill of lading or a purchase order that would provide a reason for access into the facility. That information must contain the name and telephone number of a point of contact at the facility.

The United States Military has recently employed an effective method for controlling the problems they have been facing at checkpoints in combat areas. Potential "visitors" or other groups of personnel attempting to enter an area, particularly at restricted areas such as the "Green Zone" set up in Iraq, must have their "smart card" scanned at a location several hundred yards from the main checkpoint. As a person or group of persons reaches that special location, their handprints are scanned and their picture taken. Their "smart card" is then scanned. The biometrics fingerprint information on their card and their photograph must match the scanned information in order for them to continue even to the checkpoint. That has resulted in a significant decrease in serious incidents at the checkpoints. In order to receive a "smart card" for the purpose of entering such a restricted area, one must have received the necessary clearance.

Joel Hershkowitz is Director of Marketing at Idesco Corporation. He has 26 years experience in the security industry and holds a degree in Business Management from Fairleigh Dickinson University. For more information please visit www.idesco.com.

16 **Training Articles**