International Council For Industrial Security & Safety Management

ICISS

Newsletter: February 2012

Let's professionalize the professionals…

ICISS

Security today and need of training…

Today it's significantly different! Yesterday we operated with fences, gates, guards and cameras. We were worried about people taking minor items out of the workplace. But the fences, guards and gates are not as important these days for many businesses.

An IT services company that prides itself on its relaxed and open philosophy is unlikely to appreciate a security leader whose focus is on locking the employee population out of newer communication technologies, for example. Staff and management may look at that individual as a roadblock to be surmounted rather than a partner.

Everyone would have experienced the situation while entering a luxury hotel or a shopping mall is preceded by security checks at the entry gates. The security personnel ask you to open the boot of the car and the glove compartment while another checks under the front of the vehicle with a mirror. They do not even look at a bag that you may have on the seat next to you or a package lying on the floor. The security personnel do not understand that a person wishing to smuggle explosives into the premises need not hide them in the boot, and hand guns are not necessarily kept in the glove box, as in the movies. But this is all that the guard has been trained to look at.

"We are business professionals who happen to be experts in security," stated one of the security leaders. SWOT analyses and cost/benefit analyses within the security department are important to build better performance and to better enable the security staff to "talk business." This change in attitude is making security executives more professional and are welcome to any corporate culture where they are taken as "assets" rather than as" liabilities"!

Capt S B Tyagi
For ICISS

Food for thought:

If it is not already with you, provably it will harm you: the information, the technology – in short, 'The Edge'!

Security Training: A Pre-requisite for a Secure Place

Courtesy: Col D R Semwal (callsamydr@yahoo.com)

He is highly experienced (29 years' service in Indian Army) with proven skills in managing Safety and security issues of establishments, managing large human resource deployments, logistics & mobility.

Col. Semwal has experience & passion for protection of ecology & environment. He changed the face of Delhi in Bhati Mines Area while he was commanding Eco-Battalion of Territorial Army in Delhi and turned it into lush green area!

He was successful in restoration of mining land by afforestation activities in coordination with Deptt of Environment, Government of Delhi.

He has vast experience and knowledge in Industrial Security and Safety in combination with expertise related to Environment and Ecology.

Nothing could be farther from the truth, because untrained security personnel will lull the security Department and establishment as a whole that he is supposed to protect into a false sense of security. Not having a security person would possibly persuade whole organization to take suitable precautions to cut down the level of risk. But having security personnel who are just not trained for what they are supposed to do is a potential lethal situation at the time of emergency. And, it is situation better avoided!

In the competitive world, specialist are preferred with a view on man management, keeping to minimum cost as pre – requisite to higher growth with an aim to high profit and sustainability. It becomes more important in every aspect of private security deployed in the industry; training plays not just an important role but the primary role. This is especially true for security personnel are stationed at vital installations.

Securing vital installations with high-tech electronic security or designing a complete security structure for a premise is not enough to provide foolproof security. The Security personnel working behind the machines must also be trained enough so that whole setup is considered indispensable and impregnable. Enlightened establishments are ensuring that the security professionals who take care of the security are better trained and are updated with the changing patterns of security across the globe.

Sadly, while the realization of the need for training is apparently there, ground realities indicate that even now, organizations attempt to cut costs by circumventing the training part of the entire security exercise, or at best it is turned into a crash course of sorts where just the basics are mentioned without really going into the details of what is really needed.

In other words, what is attempted to pass-off as a trained security professional is actually someone who has had a few hours crash course on what is expected of him. For all practical purposes the security professional is not trained at all. That is a dangerous situation!

Everyone would have experienced the situation while entering a luxury hotel or a shopping mall is preceded by security checks at the entry gates. The security personnel ask you to open the boot of the car and the glove compartment while another checks under the front of the vehicle with a mirror. They do not even look at a bag that you may have on the seat next to you or a package lying on the floor.

The security personnel do not understand that a person wishing to smuggle explosives into the premises need not hide them in the boot, and hand guns are not necessarily kept in the glove box, as in the movies. But this is all that the guard has been trained to look at. Most likely, he doesn't have a clue what to look for, as he has not been trained to recognize bombs and explosives and this will continue to happen until unless he has been trained on the subject.

The Government, in recognition of the fact that training is an essential component of security, has been specified in the Private Security Agencies (Regulation) Act 2005, that an agency cannot hire a guard unless he has undergone the mandatory training that has been specified. But small time private security agencies that have mushroomed across the country in recent years have made their own interpretation of the PSAR Act and started recruiting security guards with little or no training. In several cases these agencies themselves provide the newly hired recruits some rudimentary training even though they have no authority to impart this training and put the guard in uniform and post him on duty.

Security Professionals will agree that the PSAR Act needs to be more specific and clear on the concept of training and on which agency would decide what kind of, and how much training is needed for a particular security function. The security personnel as per PSAR Act 2005 need to have mandatory training for a minimum period of 160 Hrs. before deployed on duty. The security industry also agrees that they need a recognized certification authority that can decide the level of the mandatory training that is needed in the Industrial set up.

For instances, if an installer is carrying out a CCTV installation at an establishment there should be a recognized third part accreditation certifying that the person is trained enough to do the job properly. The same is the case with security guards who need more than just a uniform to be effective security guards. Industry players say that lack of specification is allowing small time companies to create training academics that neither are nor qualified to train and supply security guards.

Ex- servicemen deployed as security guard are the best trained security professional available to be deployed by the Private Security Companies in the Industry. But due to change in circumstances refresher training is must to get desired result. This is obviously due to at least in electronic security technology is advancing at such a rapid pace that refresher training is necessary to keep the security professional up dated with the latest developments.

For instance, post 26/11, lot of emphasis is being given on how to deal in with evacuation in case of Bomb threat and emergency like terrorist situation in the area that they are deployed. But the problem continues as most companies do not like the idea of investing resources such as manpower, time and money in such training due to lack of awareness.

Periodic reports have proved that in India the CCTVs installed in shopping malls or railway stations fail to catch anything of any relevance due to person responsible for supervising installation was not aware that person installing a CCTV system at their premises was skilled enough to do so or that the guard posted at their premises was trained or not. However, awareness level is steadily on the rise in metros, it still has a long way to go in smaller cities. “In India, cheap labor heralded in the concept of hiring unskilled security guards who are classified in the same bracket as ordinary manual labors and are paid by the minimum wages for unskilled labor criterion.

The Nine Practices of the Successful Security

In many professional fields—legal, technology, and finance, for instance—one can expect to find certain commonalities among the practitioners.

These professionals share certain certifications or degrees, or they've progressed through a series of common steps or training regimens to reach their current position, where they share a fairly standard reporting level. The security profession does not fit into such a mold.

However, across this varied landscape, commonalities of successful leadership do exist. Our security community comprises many individuals who are recognized in the industry as highly successful security leaders.

Nine practices have been identified that the most successful leaders have in common:

1) The creation of a robust internal awareness program for the security department, including formal marketing and communication initiatives
2) Ensuring that senior management is made aware of what security is and does
3) Walk-and-talk methodology—regularly talking to senior business leaders about their issues and how security can help
4) Conversing in business risk terminology, not "security"
5) Understanding the corporate culture and adapting to it
6) Winning respect by refusing to exploit fear, uncertainty and doubt
7) Basing the Security program goals on the company's business goals
8) Having top-level support from day one
9) Portraying Security as a bridging facilitator or coordinator across all functions

Some of these items the leaders have worked to achieve, such as creating internal awareness programs and conversing in business risk terminology. Others have come from luck or hard-won experience.

The creation of a robust internal awareness program for the security department, including formal marketing and communication initiatives

A formal marketing and communications initiative builds internal awareness of the security department and raises the understanding of what security does and the value it imparts to the organization. This is not to be confused with a security risk awareness and training program. In this case, the successful leader knows that the security department is often not understood or that many employees do not even know there is one.

The "marketing" in this case, for example, involves having an internal logo and tagline for the security department (that is, branding the department), holding brown-bag lunches with security issues infused into them, regular newsletters on security department happenings, and encouraging and rewarding employee security champions.

When employees across the organization not only recognize the importance of security's contribution but become invested in furthering it, the security function's potential for success dramatically improves.

Ensuring that Senior Management is made aware of what security is and does

Management's perception of security impacts funding and organizational support for security initiatives as well as the security leader's ability to influence risk-related decision making at a corporate level. All of these limit the effectiveness of the security function.

It will be difficult for a senior manager to develop an accurate understanding of his or her organization's security function without direct input from the security leader. Because the structure and operation of security differ so much from business to business, past experience at other companies may lead a senior manager to a view of security that is unrealistic or erroneous in his or her present environment.

In addition, because the security industry in general has done a poor job defining itself in a business context, many corporate executives continue to assume that security begins and ends with guns, gates, and guards until they are shown otherwise. What security managers often fail to do is to fully understand (or analyze) their resource capacity regarding what the security staff is spending their time on and providing on a day-to-day basis.

Walk-and-talk methodology - regularly talking to senior business leaders about their issues and how security can help

Successful security leaders take the initiative to set up meetings with senior executives as well as business unit leaders across the organization. As one leader stated, "I don't wait for the phone call; I invite myself to major business meetings around the world." Sometimes it means taking the initiative to learn business processes, especially if no one volunteers to show you the ropes. In some cases the security leader manages all these relationships himself; in others, deputies are charged with heading up regular communications with a select set of business units, making sure they understand their world and represent them in security plans.

These meetings are most effective when the security leader enters them with a business-first attitude. Note the wording of the first sentence in this section: the goals and concerns of the business leaders—not the concerns of Security—come first. Security leaders begin by asking what senior management wants and needs to accomplish, then present themselves as helpers in accomplishing those action items.

> *Security does not set the agenda; the business sets the agenda!*

Both these elements are critical to effective "walk and talk." If a security leader tries to insert him or herself into regular meetings with senior management but ignores the second lesson on the tone and content of the talk, he or she may be viewed as arrogant or micromanaging.

Conversing in business risk terminology, not "security"

"We are business professionals who happen to be experts in security," stated one of the security leaders. SWOT analyses and cost/benefit analyses within the security department are important to build better performance and to better enable the security staff to "talk business."

Even if the mission, goals, and strategies of the security function are perfectly aligned with the same in the business, if they are not communicated in the right terms, they may be rejected by senior management. The language of security is not easily translated by non-security business executives. Terms that describe security tactics, operations or projects may have double meanings—or no meaning at all—in business language.

“Perimeter” has different meanings in corporate security and information security. “Convergence” is a commonly used term in many functions whose definition varies with its speaker. Even the word “risk” has a broader meaning for business (i.e., taking a calculate risk to enhance revenue) than for security.

Understanding the corporate culture and adapting to it

Many security leaders feel it’s their job to change the corporate culture into something that is more security-centric. But successful leaders believe the opposite: Their job is to learn the existing corporate culture and find the best ways to fit security into it.

An IT services company that prides itself on its relaxed and open philosophy is unlikely to appreciate a security leader whose focus is on locking the employee population out of newer communication technologies, for example. Staff and management may look at that individual as a roadblock to be surmounted rather than a partner.

If on the other hand, the security leader talks with HR, employees and management to learn what the corporate culture values most, then negotiate security policies and solutions that leave those values intact, the perception of that leader will be markedly different across the organization.

Winning respect by refusing to exploit fear, uncertainty and doubt

Respect is won over time, so this accomplishment requires long-term improvement and consistency. While tapping into the fears of business may seem the easiest way to gain support and elicit reactions, ultimately it results in a loss of influence and trust.

The successful leaders focus on communicating risk in business terms, as something to be transferred, mitigated, avoided or accepted—not feared. If the security leader is consistently level-headed in describing risks and their implications on the business, clear in conveying the options for managing the risk, and receptive to management’s concerns and decisions, he or she is likely to earn lasting respect.

Basing Security program goals on the company’s business goals

One security leader stated, “Security enables the business to take risks—we don’t block them.” And another: “Our strategic plan is to enable the company to be the company.”

If brand protection was a major corporate concern, for instance, it became the priority of Security. Some security leaders who took this approach reported that management and other business units began coming to security to ask for assistance and advisement on various issues.

The security leader who puts the business before the function is more likely to experience long-term success than the one who works to drive the business in a direction set by security.

Communication is another factor. Basic psychology holds that a leader who is constantly asking “How can I help you?” will be met with less resistance and will be more positively perceived than one who is constantly interjecting “You can’t do that.” This positive perception easily translates into greater influence, always a factor in improved performance.

Having top-level support from day one

The success of these leaders may be as attributable to their acumen as to the clear organizational focus on security’s value. However, a caveat: If your internal success is relies on this relationship, you may be out the door when a senior management shake-up occurs. Make sure the other practices are in place to thwart immediate displacement.

Portraying Security as a bridging facilitator or coordinator across all functions

Every business unit in an organization is subject to, and sometimes owns, various risks. Man security leaders took it upon themselves to become central points of contact on risk for other business units. One stated that his organizational risk committee regularly sends information to business units to review and asks them to report back, ensuring they have an opportunity to make their voices heard.

Another remarked on his function’s close relationship with no less than seven operational functions. That leader further stated that strong security requires these business units to be engaged in risk management rather than periodically reminded of it.

When Security acts as a bridge between functions throughout the organization, it can help minimize redundancies and optimize resources. The security leader who focuses on achieving this also has the opportunity to identify, understand and respond to business unit risks more quickly.

What Does This Mean to You?

Nine common practices are identified based on research by several organizations from the collective knowledge of industry-recognized leaders, no doubt there are more.

The security function needs to share its wisdom to become a better understood, more highly recognized, and more valued contributor to an organization's bottom line.

Cartoon Corner

“Nothing’s gone wrong in the last hour. That can’t be right.”

Fighting Crime with Flower Power

Sure, most parts of the India may be headed for a long winter, but spring will eventually come! And with it comes an opportunity to fight crime.

Here's a new concept: battling the bad guys with Bougainvillea? Foil felons with Fuchsias, and chase criminals with Camellias? Can flowers actually help prevent crime at your property? The answer is "yes." Flowers and landscape plants can not only beautify your property, but can be an effective crime fighting tool as well.

Historically, we have relied on methods of security that are of the "target hardening" variety such as locks, gates and iron bars to prevent crime. These visible security devices are valuable, but sometimes limited in their effectiveness. Today, many are turning to the softer side of crime prevention, and complimenting locks and deadbolts with landscape plants, flowers and other design features to provide an additional layer of safety and security.

Crime prevention through environmental design (**CPTED**) focuses on how the environment contributes to the crime rate, and incorporates design features to remove the opportunity for crime. Crimes occur because there is opportunity for the criminal to commit the crime. Many times the physical design of one property offers more opportunity than the next for the criminal to operate. By incorporating CPTED, you can lessen the opportunity for crime, making your property a less attractive target for criminals.

The one aspect of CPTED, Natural Surveillance, is that criminals feel less comfortable in areas where they are being watched, or may be seen. Keeping shrubs and trees trimmed to maintain the feeling of openness and visibility makes the criminal element feel like they are at risk of getting caught. On the other hand, legitimate users of an area feel safer because they can see what is going on around them and can see potential threats and respond quicker. A property with overgrown and unkempt landscape is an invitation for criminals.

Natural Access Control utilizes landscape plants and other natural design elements to channel people away from unauthorized areas. For instance, a paved walkway lined with flowers strongly suggests the approved route to a proper entrance. A thorny vine or rose bush can restrict access to windows or a graffiti-plagued wall, and add beauty to the property as well. The goal of using landscape plants is not necessarily to prevent, but to discourage trespassing into unauthorized areas. This is accomplished in a more subtle way rather than overwhelming the environment with the presence of "hard" security measures.

Territorial Reinforcement is based on the idea that criminals feel less comfortable operating in areas where they perceive someone is in control. Territorial Reinforcement utilizes "Pride in Ownership" to send a clear message that the people responsible for a property take pride in it and will challenge someone coming there to commit crimes. Utilizing decorative pavers or colored concrete and freshly planted flowers to identify private property gives residents a sense of territoriality and projects the image that someone is responsible for the property. Criminals are less likely to commit crimes where they feel that there are people who take an interest in the property and will protect it.

Following are a brief overview of the four main CPTED design guidelines widely accepted by CPTED practitioners.

CPTED Principle#1 Natural Surveillance

"See and be seen" is the overall goal when it comes to CPTED and natural surveillance. A person is less likely to commit a crime if they think someone will see them do it. Lighting and landscape play an important role in Crime Prevention through Environmental Design.

CPTED Principle #2 Natural Access Control

Natural Access Control is more than a high block wall topped with barbed wire. Crime Prevention through Environmental Design or CPTED utilizes the use of walkways, fences, lighting, signage and landscape to clearly guide people and vehicles to and from the proper entrances. The goal with this CPTED principle is not necessarily to keep intruders out, but to direct the flow of people while decreasing the opportunity for crime.

CPTED Principle #3 Territorial Reinforcement

Creating or extending a "sphere of influence" by utilizing physical designs such as pavement treatments, landscaping and signage that enable users of an area to develop a sense of proprietorship over it is the goal of this CPTED principle. Public areas are clearly distinguished from private ones. Potential trespassers perceive this control and are thereby discouraged.

CPTED Principle #4 Maintenance

CPTED and the "Broken Window Theory" suggests that one "broken window" or nuisance, if allowed to exist, will lead to others and ultimately to the decline of an entire neighborhood. Neglected and poorly maintained properties are breeding grounds for criminal activity. We will work with you to develop a formal CPTED based maintenance plan to help you preserve your property value and make it a safer place.

Take a look around your property and decide if it offers added opportunity for crime. Is it an attractive target for criminals due to the lack of a little TLC, or does it project the image that care has been taken to maintain it? Remember, an overgrown Fichus tree can offer opportunity for a criminal to operate unnoticed. On the other hand, a delicate row of daisies can be a subtle but powerful guardian, protecting your property, while looking good doing it.

Reference

1. **Crime prevention through environmental design -** From Wikipedia, the free encyclopedia **http://en.wikipedia.org/wiki/Crime_prevention_through_environmental_design:**
2. International CPTED Association http://www.cpted.net/

Don't Talk While He Drives!

Suggestions & feedback may be sent to us on e-mail: captsbtyagi@yahoo.co.in

P.S. - If you don't like to receive our newsletter, we apologize for bothering you. Please let us know your mail address, we will move it out of our contact list, thank you!