



# International Institute of Security & Safety Management



*Let's professionalize the professionals...*



**Newsletter of NCR Chapter : June 2006**

## **What is needed to make security a profession – Professionalism!**

Security consciousness is nothing but the wisdom to adopt preventive or deterrent measures. It is only the concerted effort by all the members of the industries, and, all the Industries of the country, that will make the working environment in India conducive and safe.

Security consciousness is developing in India with very fast speed. The potential of growth of Industrial security management is very high and the industry based on industrial security gadgets is only developing and the modest estimate is that it is only second to that of information technology. The attitude is changing, the aptitude is changing and basically the outlook is changing with the change in the society and the law-and-order situation. Thus, today security of industries or the business establishments is more scientific and professional.

For the professionalism, the NCR Chapter of IISSM has been in the forefront in propagating the idea to develop 'industry governed' professional benchmarks for the education and training of security personnel. The recently concluded Certification course for Security Executives by IISSM is by any standard, a good indicator that the demand for high professional standards of training and education is growing and also finding recognition.

Goethe once said, "Let every one sweep in front of his door and the world will be clean!"

**This news letter contains articles –**

- **Tips on reducing false alarms**
- **While buying the security system that will protect your family...**
- **Retail Security: new line of defense**
- **France entering new age of CCTV surveillance**
- **CCTV System for highway security**
- **Benefits of creating a mentoring program**



# Professionalism in Corporate Security

Courtesy: Sudhir Gauriar ([sudhir.gauriar@bharti.com](mailto:sudhir.gauriar@bharti.com))

## About the author:

Sudhir Gauriar, a graduate in Science joined the BSF as Direct Entry Officer in 1976 and remained with the Govt. of India till 1998. In his 23 years with the Govt, he had the privilege of serving the IB, SPG and Cabinet Secretariat.

For the last Seven years, he is in the Private Sector and has been General Manager (Security) of a chain of Five Star Hotels. He is presently working as **Chief of Security in Bharati Telecom**. An Expert on Security, Sudhir Gauriar had the honor of visiting 30 countries on sensitive security assignments. He is associated with IISSM for last five years and was conferred FIISM in 2002.



Arguably there has never been a more interesting or exiting time to be security professional working today in India!

In many companies security has finally risen to the top of the corporate agenda, fuelled by the spate of terrorists' misadventures world over and explosive -mania exhibited by terrorist closer home! Today's international business climate, which is now defined by a constant and very real threat of terrorism and business crime, demands a range of relevant and integrated security solutions wherein systems and security guarding work together in harmony.

Concerns over forthcoming Commonwealth Games in Delhi and the ever present threat of terrorist attacks and regulation of private sector security have made the security profession a bit complex and challenging but at the same time professionally very satisfying and rewarding.

Speaking of Commonwealth Games, Surveillance Solutions will be highly prioritized technology applications, second being Access Control Systems which Delhi is going to need! There have been the latest developments in the world of CCTV! There are some tremendous DVRs on the market, for example, which are helping to secure convictions in the courts world-over thanks to the superb pictures they render. Mobile CCTV is also increasing in popularity, so too authentic number plate recognition systems.

In the world of access control, biometrics is finally beginning to grab the attention of the many end-users. Then there's the intruder alarms sector. Here, not only are the industrial standards in place now, several integrators are also offering alarm monitoring over the Internet.

So much fundamental transformation is taking place within Security Industry in India that coping-up the demands will make solution-providers engagement diaries obsolete and they have to opt for PDA!



# TIPS ON REDUCING FALSE ALARMS



## What is a false alarm?

A false alarm is a request for a responding authority to dispatch people and equipment where there is not an actual emergency. A false alarm can be caused through human error, faulty equipment, and misapplication of detection devices, environmental factors or simple miscommunication.

False alarms are not an exclusive problem of the security industry (in fact, by some estimates, more than 50% of all 911 calls are not crime related) however, the growing number of installed burglar alarm systems is placing an increasing demand on responding authorities (police, fire dept., ambulance).

## Who is to blame for false alarms?

The focus and blame for the false alarm problem in the trade press has jumped from one professional, or one link in the chain, to another. Two years ago, the spotlight and blame was focused almost solely on the end-user. Listen in on a seminar or read an article from that time and you would most likely encounter words to the effect, "End-users had better learn to use those security systems and cut down on those false alarms. It's not a manufacturer problem, it's not a dealer problem, and it's an end-user problem."

As the National Burglar and Fire Alarm Association (NBFAA) focused its efforts increasingly on licensing, the emphasis and blame shifted to the dealer. Dealers weren't installing the systems properly and they weren't training the end-user how to use them adequately. It then became a dealer problem.

Today, the emphasis and spotlight is shifting to the manufacturer. A column in the May 1997 issue of SDM Magazine recommends an industry approval requirement for control panels, a recommendation intended specifically to address false alarm reduction. The clear implication is that it's now up to the manufacturers to provide the answers and solutions to the false alarm problem.

Each one of these approaches is dead wrong. No single entity in the community has the ability alone to solve the false alarm problem or, in fact, to provide true security protection.

## What can the end-user do to reduce false alarms?

As the end user, there are several steps one can take to ensure false alarms are being reduced on their end. For example, the following is a small sampling of some of these ideas:



- **No dispatch period:** As with any new piece of technology, a certain degree of trial and error occurs within the first week to ten days as the end user becomes comfortable with the equipment. On suggestion is that you request from your monitoring station a specified no response period to ensure should you make a mistake; the authorities will not be called.
- **Double keystroke keypad panic buttons or a security feature on the panic button:** In the time of duress a panic button is the most effective button you could employ on your key pad or pendant. However, these panic buttons are also a major source of false alarms. Children and adults alike can accidentally trip this feature if it is one key-stroke activation. Request the double action codes (where you must simultaneously press two separate keys down).
- **Eliminate Silent Alarms:** While the silent alarm is an effective tool for catching thieves in the act, it is also a source of false alarms as the end user does not know when they have made a mistake. Installing a sounding device not only informs a thief that an alarm has been tripped, but will also warn you and your family of an error or a crisis situation.
- **One device per security zone:** Many false alarms have been caused by problems occurring after a repair has been performed. This is because the technician will have a difficult time isolating the problematic device and will sometimes repair/replace the wrong piece. By isolating each device to its own zone, the technician can quickly asses the problematic device and repair it.

---

## While buying the Security system that will help protect your family...

When considering which company will install the security system that will help protect your family for years to come, it is important you feel comfortable with your choice. After you have purchased, had the system installed and the technician has left, it is you who will live with the consequences. For this reason alone, it is very important to ask all of the right questions, so as to achieve the level of comfort you need.

### The questions to ask are...

- How long has the company been in business under the same name?
- How many system installations has the company done?
- How many installations has the technician that will be installing your system performed?
- Are their technicians up to date on all the latest equipment? What type of training do they receive?
- Will you have a say on where they install the various components of your system?
- How will they wire your system? Will wires be visible?



- How many technicians will perform the installation? How long will it take?
- What brand of equipment do they install? Why?
- Will you own your system 100%? If not, who will?
- What happens when an alarm is tripped? What happens in the event of a false alarm?

---

## Retail Security: A New Line of Defense

Loss prevention has become as important to retail profits as products, pricing and promotion," said Robert Siegel, General Manager of Video, Software and Networked Solutions at GE Security. "Retailers can preserve--and often increase--profits simply by investing in systems that reduce shoplifting and internal theft."

While shoplifting has dominated security resources, current studies question this approach. Siegel observed, "Many retailers are surprised to learn that nearly half their shrinkage is due to employee theft."

While shoplifting is one concern, it is definitely not the only one. According to Brett Birch, Africa sales leader at GE Security, a breakdown



of shrinkage in the 2002 U.S. retail market found that almost half of all losses were due to employee theft (with 32 percent from shoplifters, 15 percent from administrative error, and another 5 percent from vendor fraud). Another study, this one by software and security solution provider Encapsulon, found that "50 percent or more of shrink may be attributed to administrative and customer-service errors, plus operational issues." One example cited in the Encapsulon study describes how bottled water is sold. Frequently, more than one barcode is attached--one on the outside to signify the price of the whole box, and the others are placed on individual bottles. Predictably, these two prices vary greatly. Losses occur when cashiers make honest--or dishonest--mistakes. In 2002, for

example, U.S. retailers lost US\$31.3 billion to losses like these, according to GE's Birch.



# France Entering a New Age of Surveillance

France's anti-terrorism law, already considered one of the toughest in the E.U., has been further strengthened with the nation's deputies voting 202 to 122 in favor in December 2005. The law was brought forward by Interior Minister Nicolas Sarkozy, who said it was drawn up partly because of the bombings in the U.K. It aims to improve France's legislative arsenal to prevent a catastrophe.

Due to strict privacy laws, France has only 60,000 cameras in public places compared with 4 million in Britain, but this is set to change as the new law would allow installation of cameras in public places for the first time.

Sensitive target areas include railway stations, airports and other public areas, including churches, mosques, factories and nuclear plants. New plans allow private companies to install cameras outside premises, granting police access to all footage.

The spread of surveillance--especially in the public sector--will be mostly digital, IP-based systems with great emphasis on video analysis. Upgrades also look promising. "The extent of surveillance is already pervasive in the private sector," said Dvir Doron, Vice President of ioIMAGE. "This new development is expected to drive the video market in the public sector. Nevertheless, we believe that this is not going to be a grudge purchase. Decision-makers are asking what measurable results they can get out of additional use of surveillance." Just adding more cameras, he said, is not enough. Adding a layer of intelligence could make video much more effective.



Many factors need to be considered when building new systems, especially ones as large and complex as those used by governments. Guaranteeing utmost flexibility and compliance with existing and upcoming solution architecture is important. "Video requirements will always vary," said Jean-Luc Asael, Commercial Director of Dallmeier, France, "but they aim at achieving extensive, tailor-made, all-around solutions that meet the highest-quality security requirements. Besides excellent picture quality and easy operation, the No. 1 demand is for compatible, flexible system architecture for easy integration into existing security-management systems." A flexible design, he continued, enables expansion at any time and possibility of adding further alarm systems or integrating them into higher management systems.

Under the new anti-terrorism law, official snooping of Internet and mobile-phone records will also be permitted. Detention periods for suspected terrorist will also be extended. Internet and mobile-phone operators, for example, will be required to keep records of client connections for one year and officials will have greater authority to conduct identity checks on cross-border trains and automatically monitor vehicles.



Civil rights groups and left-wing opposition parties have expressed concern over the law, which they fear gives authorities too much power to invade citizen privacy and confuses immigration and terrorism, according to French press agency Agence France-Presse.

---



## CCTV System for Highway Security

In the past, CCTV systems were used principally facility observation and surveillance. They were used for industrial application as well as production and process monitoring in high precision and highly vulnerable industrial processes. They were also used in airport and prison security.

Now CCTV Systems are also being used for controlling traffic flow to reduce congestion. With the development of new high-resolution CCTV camera systems with fast pan, tilt and zoom functionality and built-in auto-tracking capabilities, systems now add an extra dimension to road safety by providing fast identification of potentially hazardous situations and fast accident recognition.

CCTV systems designed for road and traffic surveillance have to contend with an exceptionally broad range of challenging situations--from monitoring high-speed intercity highway traffic to surveillance of crossroads and pedestrian crossings on relatively slow-moving urban roads. They also have to deal with varying visibility due to weather and changes in road lighting, which can vary from bright daylight to twilight to artificial lighting at night and within tunnels to even unlighted roads. Automatic character recognition is also becoming essential for identifying vehicle registration-number plates. Thanks to advanced technologies almost every problem can be solved so surveillance systems can work more effectively through intelligent cameras and flexibly via network infrastructure.

---

**“Do what is right - for that reason alone!”**

**- Charvak**

---



# Benefits of creating a mentoring program

Courtesy: Rajiv Mathur, CEO, Vision Security ([rmathur.vision@gmail.com](mailto:rmathur.vision@gmail.com))

## About the Author:

Rajiv Mathur is a seasoned professional with about 15 years of experience in the industry. A Management graduate in Human Resource and Marketing, he has also acquired additional qualifications in the field of Information & Systems Management.

As a **CEO of Vision Security**, he believes in Knowledge based management of a field force of about 5000 security personnel and 16 offices across India. He has been instrumental in getting ISO certification for the organization. Training is the key interest area and has presented papers on various subjects at different national & international platforms.

A keen learner with dedication & innovation as the success mantra; is also called "The Professor" by his friends and colleagues. He is also Joint Secretary of the NCR Chapter of IISSM.



There are many benefits of creating a mentoring program in your organization. In her book, *Mentoring for Success*, author Elizabeth Weinstein, PhD, lists several advantages for

introducing mentor-mentee relationships into the workplace:

## Healthy Work Environment

- Helps support the organizational mission.
- Encourages creative ideas to flourish.
- Enhances cooperation and establishes a foundation for effective teamwork.
- Improves communication between different levels in the organization.

- Helps employees adapt to the changing workplace by sharing information, concerns and possible

## Strategies for addressing issues

- Makes a statement about the organization's values.

## Leadership Development

- Develops future leaders, resulting in effective succession planning.
- Creates an opportunity to promote and retain employees with leadership potential, especially

## Women and minorities

- Enables future organizational leaders to develop and practice skills.
- Motivates mentees to work towards being effective leaders. Cost Effective
- Results in increased productivity because of the improvement in employee skills and motivation.



- Reduces organizational turnover. Mentees receive individual attention and plan for their careers in the company.
- Requires minimal time commitment.
- Makes hiring of new employees more cost effective if young people can be mentored in intern positions and gain the appropriate training before becoming an employee.
- Requires a low financial investment.
- Uses talent that might not have surfaced otherwise.

### **Diversity**

- Advances capable individuals, particularly minorities and women.
- Helps organizations to meet diversity goals.
- Assists in retaining the "balance" of the organization. Mentees bring a variety of experiences and backgrounds that enrich the organization.

### **Training**

- Enables new hires to be easily assimilated into the organization.
- Reduces the need for scheduled skill development training opportunities.
- Provides on-the-job training.
- Encourages employees to be active and life-long learner.

In addition, there are also benefits for individual mentors and mentees.

### **Mentor Benefits**

- Develops skills in coaching, relationship-building, consulting and teaching.
- Helps to rejuvenate the long-time employee.
- Assists in decision making by seeking the mentee's perspective and input.
- Validates the skills and experiences gained, which provides a sense of achievement.
- Creates a feeling of knowing that the mentee is learning and growing. Mentee Benefits
- Allows the opportunity to try out new ideas using the mentor as a sounding board.
- Provides career development planning.
- Absorbs the new hire into the organization.
- Help to identify skill development needs and seeks alternatives for meeting those needs.
- Learns about the organizational culture (policies, procedures, systems and relationships).

---

**“The success comes not with the absence of conflict ...  
... but with the ability to cope with it”  
- Kautilya: Niti Shashtra**

---



"The virus was contained in an e-mail warning about the virus . . ."

---

## Epilogue:

The field of security management in India is still in the stages of growth and evolution. Many changes have occurred over the past several years and surely many more are in store in the years ahead!

Even the term used to label this professional field, let alone, the definitions used have undergone changes. Are the security professionals involved with security, safety, and loss prevention or risk management? The correct answer is "all the above"! As the field becomes more professional, the duties of the security practitioner become more complex and encompass a far wider range of responsibilities. No longer is security saddled with a night watchman's image!

**Security professionals are therefore urged to read more, write even more and develop the fraternity, for there will be help available from within! Need not seek it from outside!!**

---

**Suggestions & feedback may be sent to us on e-mail: [captstbyagi@yahoo.co.in](mailto:captstbyagi@yahoo.co.in)**

---