International Council For Industrial Security & Safety Management

Newsletter: December 2011

Let's professionalize the professionals...

http://www.wix.com/sbtyagi/iciss

Better Security Sense...

The most essential quality, which we have but ignored, is the power of observation.

We see but we don't observe. Observation is not just seeing thing but understanding the implications of what we see. So effective observation of what goes on around us is a very important requirement for better security sense. Wherever you are, be it at home or outside in a public place look around and try and see through things rather than just see them.

Try and gauge the need for a thing to be present at a particular place, for a person to be standing at a particular place. Don't ignore anything that seems unusual. Pry harder and you will come out with surprising results. Make observation a habit.

Capt S B Tyagi
For ICISS

The Leadership Principle:-

They, who would give up an essential liberty for temporary security, deserve neither liberty nor security.

Benjamin Franklin:

Digitally signed by Capt SB Tyagi, COAS'CC
DN: cn=Capt SB Tyagi, COAS'CC, o=International Council of Security & Safety Management, ou=Co-founder, email=sbtyagi1958@gmail.com, c=IN
Date: 2011.12.01 14:05:06 +05'30'

The Domain of Security From International to Human

Before my joining as a Security Executive, I served as a Commissioned Officer with the Indian Army. During my service, I got the opportunity of deployment at Indo-Bangladesh border, Indo-Pakistan border, Indo-Myanmar border and Indo-China border. These ground scenarios taught me to define security as protecting the political and physical integrity of sovereign nations like that of our country.

In its traditional form, security is centered on the preservation of the sovereign state from external threats and the activities of other states. It thus requires internationally recognized boundaries protected if necessary by military action, prohibition of the use of force between states and non-intervention in the affairs of other states. Under the UN Charter, individual state security is supported by collective security. The Security Council's primary responsibility is to maintain international peace and security. The Security Council can authorize the use of all necessary means in response to a breach of the peace, threat to the peace or act of aggression. The 'collective security' is defined simply as the Security Council, rather than as any broader community of states or other interests. The veto ensures the agreement of the five permanent members in any such collective action and is thus a safeguard against contested action. The decision to use the veto is political. Well, these were my learning when I was trained in the Officers' Training Academy of Indian Army and thereafter serving at International Borders of our nation.

But soon after I joined my new assignment, I saw and learnt a different aspect of security. Though we name it as Industrial security, but it can always be seen in conjunction with Human Security. This includes almost everything from Infrastructure, Installation, Perimeter, Access control, Township security to all sorts of employee insecurities and so on and so forth.

Coming to the International security it is assumed that the action of one or more states that threatens the security of other state(s). This means that less attention has been paid to the role of non-state actors, such as terrorists, extremists, in generating insecurity. However in the context of terrorism this has now changed. For example post 9/11; the UN Security Council recognized terrorist acts as constituting a threat to international security.

Human security denotes individual freedom from basic insecurities, whatever the root of that insecurity may be. It is also caused by internal conflict, by collapse of state institutions and vital installations like that of ours. It also emanates from violence and abusive actions by non-state actors like the present day scenario of Terrorism and Naxalism. Human insecurity is also caused by violations of economic and social rights such as the right to food, health and housing, as well as civil and political rights such as fearing torture, deprivation of life and liberty. However although denial of human rights contributes to human insecurity and human insecurity generates further violations of human rights, it is a wider concept than human rights. It encompasses physical security, economic security, legal security, political security, food security, gender security and relational security. Human security is perhaps best summarized by the inclusion of 'freedom from fear' and 'freedom from want' among the four freedoms proclaimed by President Roosevelt during World War Two. The Report on the Commission on Human Security, May 2005 added that it also includes the freedom to take action on one's own behalf, which is the enjoyment of

autonomy and self-esteem. Human security thus goes beyond and supplements international security.

Human security does not depend upon international law's distinctions between conflict, military action, internal affairs and police action. In so-called post-conflict situations, the forms of violence typically mutate from conflicts like bombings, military attacks into criminal violence like murder, looting, abductions, kidnappings, corruption, armed crimes, organized crime etc. Where the state government cannot guarantee security within the state, other actors may assume that responsibility, for example an occupying army or international peacekeepers like Indian Army is doing Peace-keeping in Lebanon, Somalia, Congo etc. However such bodies tend to perceive security within state security terms or in terms of the security of their own forces rather than in that of the human security of civilians within the state.

To summarize we can say that security in any form or at any level does not have a measuring yard and the threat cannot be calculated correctly. Hence the task of a security man at any level is important and challenging. But when the security measures are practiced by one and all, it gives confidence to security professionals to make sure that security is for everybody!

Some steps you can take while transacting online to ensure security

While all banks have made all efforts to ensure security for the customer's interest, listed below are some tips to ensure maximum security:

1. TIPS WHILE USING YOUR H-PIN

- **Change your HPIN** after your first login and change it at least once a month
- **Change your HPIN** after you access Citibank Online Internet Banking **using shared PCs**
- **Destroy the HPIN** mailer after memorizing it
- **Keep your HPIN a secret** and don't disclose it to anyone (including bank employees)
- **Do not write the HPIN** on your ATM/Debit Card or Citibank Credit Card.
- **Do not hand over** your ATM/Debit Card or Credit Card to anyone.
- **Do not use common names as HPINs** - choose passwords that are difficult for others to guess
- **Use a different password** for each of your accounts.
- **Use both letters and numbers** and a combination of lower case and capital letters if the passwords or HPINS are case sensitive

2. SCAM E-MAILS AND WEBSITES

- **If you believe that someone is trying to commit fraud** by pretending to be a concerned banks' business associate and such activities raise doubts, please contact the concerned bank immediately.
- **Be alert for scam e-mails**. These are designed to trick you into downloading a virus or jumping to a fraudulent website and disclosing sensitive information.

- **Beware!** Phony "look alike" websites are designed to trick consumers and collect your personal information. Make sure that websites on which you transact business post privacy and security statements and review them carefully.
- **Verify the address of every website, known as the URL.**
- **Make sure that the URL you want appears in the "address" or "location" box on your browser window**. Some websites may appear to be legitimate but actually are counterfeits. Take a few extra seconds and type the URL yourself.
- **Don't reply to any e-mail that requests your personal information.** Be very suspicious of any business or person who asks for your password, passport details, other banks details or some other highly sensitive information.
- **Open e-mails only when you know the sender.** Be especially careful about opening an e-mail with an attachment. Even a friend may accidentally send an e-mail with a virus.

3. TIPS WHILE USING E-COMMERCE WEBSITES

Many e-commerce websites utilize state-of-the-art encryption and other security procedures to give you a convenient and secure shopping and banking experience.

- **If you suspect a website** is not what it purports to be, leave the site. Do not follow any of the instructions it may present you.
- **Ask yourself if the information you are asked to provide makes sense** for the activity you are engaged in. For example, an online auction site should not ask for your driver's license number or the PIN for your credit card. If a site or e-mail asks for information that doesn't feel right, do not respond.
- **Keep a Paper Trial.** Print out the "address" of the company site you are on-it's Uniform Resource Locator (URL). The URL ensures that you are dealing with the right company. It's also a good idea to print out a copy of your order and confirmation number for your records.

4. GENERAL PRECAUTIONS

- **Look for the padlock symbol at the bottom right of a web page** to ensure the site is running in secure mode BEFORE you input sensitive information.
- **Make sure your home computer has the most current anti-virus software**. Anti-virus software needs frequent updates to guard against new viruses.
- **Install a personal firewall to help prevent unauthorized access to your home computer**, especially if you connect through a cable or DSL modem.
- **Log off. Do not just close your browser**. Follow the secure area exit instructions to ensure your protection.
- **Do not keep computers online when not in use.** Either shut them off or physically disconnect them from Internet connection.
- **Monitor your transactions**. Review your order confirmations, credit card, and bank statements as soon as you receive them to make sure that you are being charged only for transactions you made. Immediately report any irregularities.
- **Regularly download security patches** from your software vendors.

New Technology Application

The Super Trackstick is the perfect tool for individuals, law enforcement and government agencies looking for a way to track anything that moves. The Super Trackstick records its own location, time, date, speed, heading, altitude and temperature at preset intervals. With over 4Mb of memory, it can store months of travel information. The included magnetic mount makes the Super Trackstick easy to attach and remove from any metal surface. It has seamless integration into Google Earth™

How it works

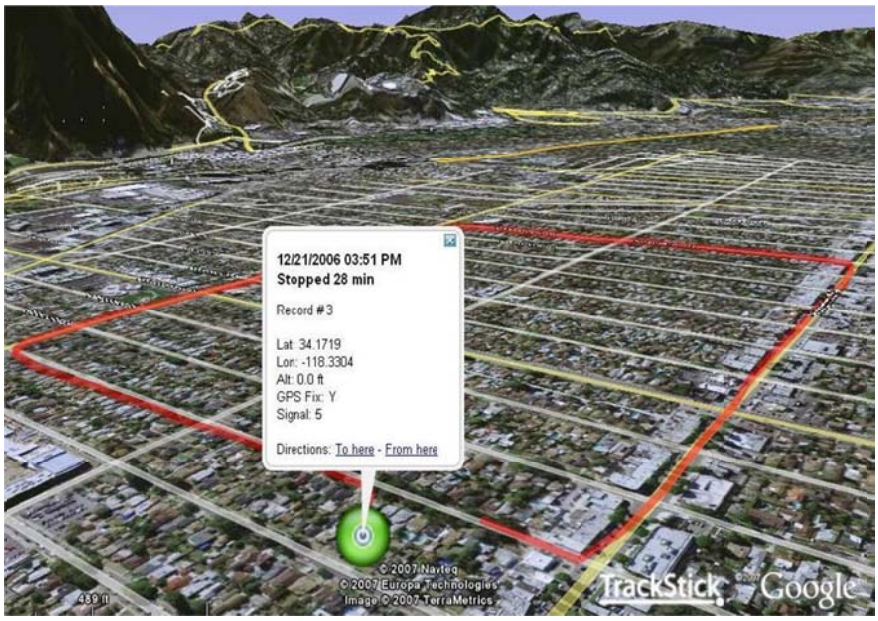
The Super Trackstick receives signals from twenty four satellites orbiting the earth. With this information, the Trackstick Pro can precisely calculate its own position anywhere on the planet to within fifteen meters.

Where it works

The Super Trackstick will work anywhere on the planet Earth. Your exact location and the route traveled can be viewed and played back directly within Google Earth™. Everything is included and there are no monthly fees.

Applications / Features

- Professional GPS location Recorder
- Vehicle location and route histories
- Package / container shipment history
- Employee and vehicle monitoring
- Mileage recording and verification
- Homeland Security
- Search and Rescue
- Military Operations
- Private Investigation
- Public Safety
- Law Enforcement
- Child / Family Safety



Route recorded with Super Trackstick in Burbank, California

The Managements' Questionnaire

How positively are the 'new' Security Officers perceived by the clients?

In retail marketing, shrinkage is a problem faced by the security professional world over on daily basis. Loss prevention is one criterion used by the management to evaluate the effectiveness of the security professionals hired by them. Certain check list therefore in order which can be used for performance management of security professionals. Following factors might be helpful to do the same -

Is the officer proactive in terms of loss prevention?

Managements recorded a 75% improvement here, attributing this to training, support, targets given to officers and their change of attitude.

Is the officer aware of store losses, and does he/she assist in reducing them?

Although the actual unknown losses measured during the trial did not show an improvement, Managements were impressed with the officers' desire and knowledge to assist in reducing such losses. The survey recorded a 119% improvement in awareness of store losses, and a 46% improvement in security officers' ability to reduce stock losses.

Are security officers adding value in tackling till losses?

This showed an 80% improvement, with 11 stores recording improved net losses during the trial. Managements are now involving officers at till-focused meetings, and sharing all data.

Is the security officer an overt deterrent to potential thieves?

Overall, there was a 30% improvement, with Managements rating the service 'satisfactory' prior to the training and 'very good' or 'excellent' afterwards.

Does the officer communicate effectively with Management?

By helping security officers to understand basic management skills and the rudiments of loss prevention, they were then able to communicate more effectively with managers. There was a measured 55% improvement here. However, it was recognized that some officers were still struggling and would need extra assistance.

Is the officer a valuable member of the store team?

Managements rated officers as valuable members of the store team, recording a 45% improvement.

Have the officers raised security awareness in your store?

Managements believed that officers had consistently helped to raise security awareness in their stores and significantly improved overall security, with many officers attending staff

meetings and helping staff to understand how they could help improve security. Managements were also impressed with the way in which officers carried out their duties, and with their personal commitment to the manager and store.

Overall, these results – taken together with the quantitative data – demonstrate that by training officers on loss prevention there is a measurable improvement in their performance that adds value to the security guarding role and justifies client expenditure.

Best Value for Business: an industry-wide strategy

Although security is typically viewed as a drain on the bottom line, there are many ways in which it can – and often does – add value to the host business. Modern security management should envision security as integral to all activities within the organization, and not as a separate function 'living life on the edge'.

The value of security can be loosely categorized into hard and soft benefits. Hard benefits pertain to the quantifiable aspects of security, and can usually be described in financial terminology. Soft benefits are equally important, but are somewhat more qualitative. They describe the more intangible benefits of security.

Ultimately, the security sector desperately needs to develop a strategy – both internally and externally-led – that will cement its rightful place at the top of the organizational agenda. That strategy must be holistic, take account of each and every threat to all organizational processes and be completely aligned with corporate objectives.

Theft by Employees in Retailing Industry

Employee Theft from a retail store is a term that is used when an employee steals merchandise, food, cash, or supplies while on the job. However, in the eyes of the law, employee theft is just theft…the elements of the crime are identical. To commit theft, the employee must "intend" to permanently deprive their employer of the value of the item stolen.

Employee theft can occur just like shoplifting by concealing merchandise in a purse, pocket, or bag and removing it from the store. It can also occur by stealing cash, allowing others to steal merchandise, eating food, and by refund, credit card, or check fraud. Employee theft can sometimes be charged as embezzlement due to the trusted fiduciary status of the employee. All of these methods lead to loss of inventory (shrinkage) and/or profit for the merchant. Employee theft is an insidious crime because the merchant is paying a wage and benefits to the thief on top of paying for the cost of their dishonestly.

In European countries where the retailing business has already seen the boom and is stabilized relatively, the Retail loss prevention is a professional diversification of security professionals that is responsible for reducing inventory losses inside retail stores. Loss prevention professionals manage in-store security programs that focus on reducing inventory losses due to employee theft, shoplifting, fraud, vendor theft, and accounting errors.

Like others in the security industry, retail loss prevention professionals must interact with store personnel and store customers when dishonestly or carelessness occurs. As you can

imagine, accusing someone of dishonestly or carelessness is not a small matter and must be done with the utmost care and professionalism.

In India too this trend is sure to set-in! The proliferation of malls and mega-stores such as Spencer's, Wal-Mart, Reliance and Big Bazaars sharply focus the need of such specialist security professionals and for the response from protection profession - time is now!

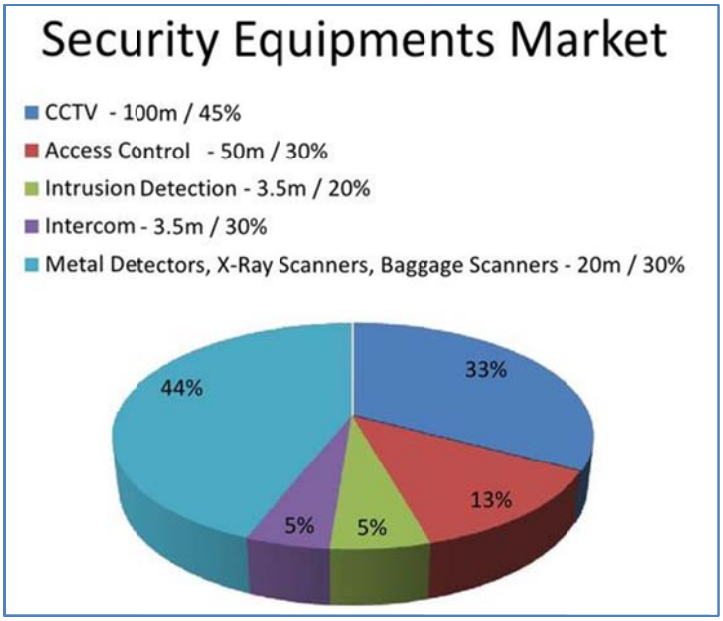
Home security market in India

Today our country is on a road to development starting many l energy ventures and critical infrastructures which will go a long way into developing our national security. The present security situation portrays a grim picture, asserting the need to di-risk and safeguards such assets and ventures. Thus

India in the year 2009-2010 spent Rs.59052.95 crores on homeland security protecting 1.2 billion people. The market segment of security solutions and man guarding combined was around US$ I.57 billion for 2010 and the major sectors were airports, mass transport and maritime. This market is estimated to be UD$9.7 billion by year 2016. The Indian electronic security market is growing at 23% CAGR with potential to grow at 40%.

The organized players comprise only 20% of the market but account for 80% of the revenues and is indicative that the large part of the market is still untapped by the organized lot.

Indians have been splurging huge money on securing their houses and new-found wealth, pushing demand for security gadgets by over 50% to Rs1, 200 crores. Burglar alarm systems, video surveillance and door-phones, access control, wall mount air sensors, motion detectors, two- way key fobs, Wi-Fi camera, wireless external siren and wristband transmitters are some of the ultra-smart devices that are in demand with increasingly affluent Indians.



"While the total security market is growing at the rate of 25-26%, the real estate and residential security market is almost double at almost 52% annually," said Director (Security) of Honeywell, South Asia.

The real estate security market is worth Rs1200 crores and the security gadgets industry is expecting to piggy back on this growth, it is said. Manufacturers' unveiled nearly 25 new products at a security fair - IFSEC India-2008 - that underlines the demand for home security and automation devices. "Also, 30% of the stalls at the fair were visited by real estate developers and individual end users who wanted security and home automation

devices," IFSEC India-2008 project coordinator said. This year more than 280 world leading companies from 23 countries (26% more than 2009) are likely to be present highlighting the burgeoning business in the field of industrial security management. There would be 11,341 Government and security professional from 43 countries in this event which shows the size and importance of the home security market of India.

The growth drivers of this phenomenal market are government sector, corporate sectors and retail and residential sectors. This market is import driven to large extent but seeing that the initial Indian entrepreneurs and corporates who ventured in the field of local manufacturing of hardware, system components and developing software, have been rather successful in short time, others are encouraged to follow suit.

A bit of adhesive is all that's needed to steal from ATM

Beware if the ATM screen goes blank after you swipe your card. It could be a mischief by fraudsters to withdraw cash from your account after you leave the ATM in a huff. A bit of adhesive and a screwdriver are all that's needed to outwit hi-tech safety gadgets.

These swindlers are part of a powerful inter-state network spread across the country. Assam Police and Kolkata Police have recently rounded up three swindlers who have mastered the tampering of ATMs. The trick applies only to ATM machines that need a customer to insert and extract the card to start operations (as opposed to ATMs where the card pops out after the transaction is complete). Many nationalized banks, including SBI and Bank of Baroda, use this system at their ATMs, most of which are unmanned.

So, what is this low-tech, highly effective modus operandi? Fraudsters, who generally strike in pairs, enter ATM by swiping valid debit card at the gate, press down a key on keyboard and stick it with adhesive so that it does not return to its original position. This switches on the machine. They then walk out and wait for a victim to step into the trap! When a customer enters the ATM and swipes the card, he does not realize that the machine is already on. A message flashes for him to key his PIN, which he does. But since the machine has been switched on in an improper way, the screen goes blank automatically as a security feature to stop fraudulent withdrawals.

The customer thinks it is a system fault and gives it a second try. He has no clue that the two 'customers' getting impatient outside are actually criminals waiting to steal his money. They start abusing him for taking too much time and force him to leave in a huff. Exit customer, enter fraudster. They simply use a screwdriver to 'release' the key. The ATM restarts automatically. What it has in store is PIN of the last customer who swiped his card. The gang enters the amount and walks out with cash.

The SBI has been receiving several such complaints. "We were at a loss to locate the fraud because the CCTVs showed the customer swiping his card. But customers complained that they couldn't withdraw money," an SBI official said.

Times of India, New Delhi Edition

Suggestions & feedback may be sent to us on e-mail: sbtyagi1958@gmail.com

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