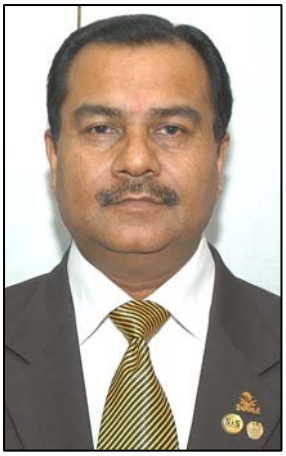
International Council For Industrial Security & Safety Management

Newsletter: April 2011

Let's professionalize the professionals…



A widely referenced definition of privacy is that "privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others"

If we accept this definition and look at the current state of affairs, then it becomes quickly clear that today we have very little control over information about ourselves. The use of surveillance techniques such as CCTV, but more importantly, techniques summarized under the term data mining, is so widespread that it can be argued that we live in 'surveillance societies'.

The dramatic rise of surveillance by means of data mining techniques, sometimes called 'dataveillance', gets 'explained' by the growing adoption of information and communication technologies (ICT). But that in fact does not explain anything. It is important to understand that the use of surveillance techniques for reasons of government and commerce is much older than ICT. The difference now is that the information society is a society which makes itself uniquely dependent on those technologies. For almost every social problem there is assumed to be a fix involving ICT.

This way of thinking is based on foundational myths of the information age which developed during the formative period of industrial capitalism.

Surveillance and dataveillance are now carried out for a myriad of reasons and are in a way 'systemic' that goes far beyond invasion of privacy alone. Data mining is not merely a passive action of preventive accumulation of knowledge but the basis of a widespread technique called 'social sorting' whereby semi-automated decision making processes define access to services and goods. The gathering of personalized information therefore is not an unwelcome by-product of technology but a key element of the way modern mass societies under capitalist conditions work.

Capt S B Tyagi
For ICISS

Capt S B Tyagi, COAS' CC*, FISM, CSC, CSP

Digitally signed by Capt S B Tyagi, COAS' CC*, FISM, CSC, CSP
DN: CN = Capt S B Tyagi, COAS' CC*, FISM, CSC, CSP, C = IN, O = GAIL (India) Limited, OU = Deputy General Manager (Security)
Date: 2011.03.30 13:47:55 +05'30'

Privacy Encroachment : What ar the issues?

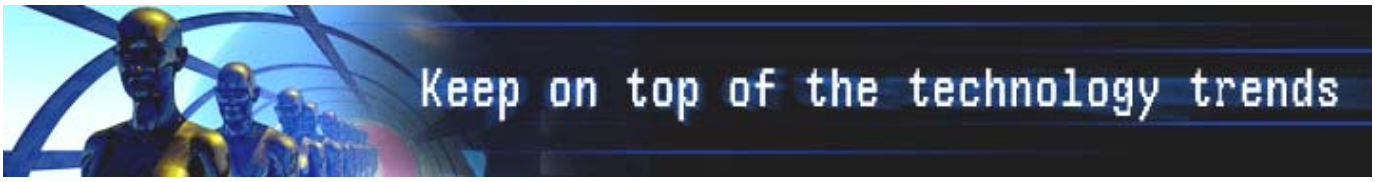
A whole range of social actors are fighting the erosion of privacy - ranging from national privacy campaign groups such as ‘Foebud. e.V’ in Germany, ‘Quintessenz’ at in Austria, the EFF and ACLU in the USA, to the European umbrella organization EDRI. Some of those privacy campaign groups are organizing the annual 'Big Brother Awards' (BBA), where the worst anti-privacy measures are 'honored' with the BBA. In Great Britain, where the BBA was invented, the physical object awarded to the anti-privacy offender is a statue of a military boot stamping on a head.

The efforts of privacy campaigners are, while well intentioned and in individual cases quite successful, are bound to fail. The jackboot is not an image that people living in liberal democracies associate with their reality. In order to develop effective strategies against the erosion of basic rights such as privacy, we need to understand what privacy stood for and meant in the historic context when it emerged as an important social category, and we need to understand the current overall political, economic, technological and socio-cultural dynamics of our time.

In 1792, inspired by the French Revolution, the London Corresponding Society started to meet in taverns and private houses, bookshops and cafes to read revolutionary literature and demand political reforms such as universal suffrage. Other popular societies were set up in regional centers such as Sheffield and Norwich. These 'English Jacobins' placed high value on self-education, egalitarianism, rational criticism of religious and political institutions, a conscious republicanism and a strong internationalism. They adopted forms of grassroots self-organization such as rotating chairmanship and organizational transparency. The ruling class reacted through the suspension of habeas corpus in 1794, followed by the Seditious Meetings Act and the Combination Act of 1799.

The revolutionaries were driven leftwards and underground. Although politically defeated for the time being, their attitudes and practices pre-configured many aspects of the political consciousness and forms of organization of later trade unionism and working class activism. After the end of the Napoleonic Wars, working class activism re-emerged and working class writers and readers created a Radical reading public. The working class ideology which matured in the Eighteen Thirties put an exceptionally high value on the rights of the press, of speech, of meeting and of personal liberty.

The process of industrialization saw the creation of large factories whose design primarily served the aim of keeping workers under control. A specific version of technological progress was set in motion, which sought direct control of workers at the site of production and the displacement of skilled human labour through machines. "It is a result of the division of labour in manufacture that the worker is brought face to face with the intellectual potentialities of the material process of production as the property of another and as a power that rules over him," wrote Karl Marx. Despite many changes in the world since then, those basic tendencies have remained the same or have only intensified.



Central Monitoring Stations

The alarm monitoring and response is very complex and tedious function of security management. Fraught with False Alarms and resource-mobilization, alarm monitoring also means that systems need to be constantly upgraded and procedures checked. There is also need to constantly audit the efficacy of the system, return-on-investment and the integrity of the data for very efficient alarm monitoring. Since all these activities occupy lot attention and priorities of the organizations, the forward looking managements started off-loading these activities to third-parties – specialist in the field. This turns out to be cost effective and very dependable option which enhances the level of security preparedness.

Security systems send their signals over telephone line to a central monitoring station- the facility that acts as the link between homes or any premises and the police, fire department, and emergency response authorities. A central monitoring station is manned 24 hours a day, 7 days a week by highly skilled operators trained to respond to emergencies. The station operator alerts the proper authorities and dispatches help.

Central Station software has to meet very special requirements processing and storing very large amounts of data and integration with many different alarm protocols. Incoming signals are processed by digital alarm receivers; these convert the incoming event packets to serial or TCP packets which are then analyzed by the Central Station software. Event packets can be communicated over any transmission medium: PSTN, GSM, Radio, direct line, Ethernet, GRPS, etc.

Spearheading this phenomenon are few security agencies in some metros in India, where they established their Central Monitoring Stations. These metros cater to big offices, industries as well as individual residents who wish to avail their services. The field is wide open and new entrants will have head start and surly benefit from the lead taken by them.

"Licensed" companies typically offer higher levels of service and reliability because they are mandated to follow certain regulations.

In Australia Central Stations are graded on 2 areas: operational and physical performance. Operational performance includes the ability of the monitoring system to respond to events - generated by customers' security systems, operational reliability, data retrieval, etc. Physical performance includes measures such as the construction of monitoring rooms - most high security rooms have airlocks which can only be operated internally. The highest standard is 1a to 3c. To be graded at 3c central stations still meet very high standards.

There are no such requirements in India and PSAR Act 2005 has no reference of such services and need for licensing thereof.

Transitioning Alarm Monitoring from In-House to a Third Party!

A monitoring center must provide timely, consistent, high-quality services utilizing state-of-the-art technology to customers 24 hours a day, 365 days a year. Keeping pace with the changes in technology and maintaining alarm system data integrity were crucial to maintaining goal of providing best-in-class alarm monitoring service.

In addition to equipment needed, enhancing alarm data integrity is also necessary to ensure the highest level of security is continuously maintained. The planning phase may include five critical elements which would become foundation to successfully convert in-house alarm monitoring platform to a third-party supplier:

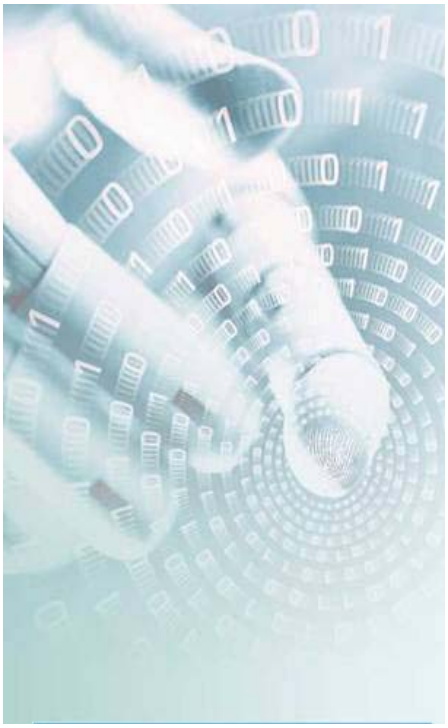
- Transition team identification
- Decision process to determine the service provider
- Project planning
- Implementation
- Post implementation (continuous improvement)

Transition Team

To successfully convert alarm monitoring to a third-party supplier, a transition team of customer-focused leaders may be selected to design, analyze, and implement the alarm monitoring transition project. In addition to loss prevention, transition team is to include stakeholders from the following departments: procurement, finance, business unit leaders, IT, real estate, legal, facilities, and operations etc. This team must meet regularly, defining the objectives, building success criteria, creating performance metrics, and representing the organization to ensure a seamless transition of alarm monitoring.

Any plan for the alarm monitoring transition may include:

- Understand the buy – interview stakeholders
- Establish operating procedures for supplier
- Develop draft scope of work for review by stakeholders
- Present sourcing strategy (scope of work, list of suppliers, and timeline)
- Develop, distribute, and analyze request for information
- Complete supplier bid meetings and site visits
- Suppliers complete and return request for information
- Present request for proposal (RFP) supplier short list recommendations to stakeholders
- Analyze RFP
- Negotiate with suppliers
- Present overview to stakeholders
- Notify suppliers and stakeholders of contract award
- Execute contract
- Develop performance metrics
- Establish quarterly performance meetings to review and track performance metrics



Determining the Service Provider

Collectively, transition team needs to identify suppliers that provided the most comprehensive, customer-focused capabilities. Criteria for a successful service provider are as following:

- Fitness to technical and functional requirements
- Total cost of ownership
- The ability to support current and emerging equipment
- Industry reputation and experience
- Experience and qualifications of the company and resources
- Quality assurance commitment
- Financial strength
- Proven methodologies, tools, and value added services

Sourcing decision must be based on the “best value/total cost” principle. While cost remains a critical decision factor, the quality of the equipment, and operating efficiencies would be the primary and most critical aspects.

Project Planning

A project task list can be created to identify key issues that can affect the overall project and allow assignment of tasks. Tasks can be assigned milestones in the project file to help balance workload for project planning. Clear communication, precise operating procedures, and partnership with selected solutions provider are the building blocks of our transition plan.

Implementation

Converting alarm system monitoring, whether from in-house to third party or third party to in-house, requires absolute understanding of a defined scope of work. To implement the alarm system monitoring change, the data from the existing monitoring facility can be gathered and scrubbed to determine its accuracy and freshness. The data then need to be formatted in order to be inserted into new monitoring systems and reviewed again for accuracy. Once all data is in place in new monitoring systems, the stage is set to develop the schedule for the change over.

Post Implementation – Continuous Improvement

The alarm monitoring conversion from proprietary monitoring platform to the Third party Monitoring Center has to be a seamless, successful event. Metrics need to be assigned to all the alarms and responses. Each metric was assigned a target goal, for example 90 percent of burglar alarms within 60 seconds. To ensure continuous improvement, it is advisable to develop quarterly performance business reviews. Business reviews provide the avenue to assess performance metrics, identify opportunities to strengthen partnership, and continue to focus on achieving both organizations' internal and external goals.

CCTV: Fundamental Flaws and Potential Improvements

The CCTV systems have one fundamental flaw – despite putting up large numbers of cameras to maximize the coverage of an area, we seldom have anybody actually looking at much of the area for which we are responsible.

Sure, we can always go back and look at what happened, but many times this just is not good enough. It is a problem of logistics and economics. We cannot staff the control room with enough people to view the number of cameras we have available. So we have many of these cameras' views going to waste when it may be useful to view them. To make it worse, much of what is displayed on monitors will be uneventful, or sometimes even have content that is irrelevant to the risk profile of the site. This problem of coverage is not likely to go away soon. However, there are technologies being implemented now or in the near future that will change the risk coverage by CCTV significantly.

Intelligent technology that is being developed can help in a number of ways. Central to this is

technology that can work with the operator in the background performing intelligent analysis of the camera views.

- Firstly, the computer can do things that computers are good at, and free the operator up to concentrate on other duties. For example, where automated recognition such as face recognition or number plate recognition can do the job, it frees the operator up to concentrate on the more relevant things that only people can do. In this way it is optimizing the use of the system.
- Secondly, background sensing and alerts or alarms allow the detection of suspect conditions on cameras that are not currently being viewed by the operator. The computer can highlight these or bring these to the operators' attention for viewing and investigation. This could include certain types of movement or the presence of somebody or something in an area for defined periods. Through this, the coverage of the cameras has been made more efficient.
- Another option is acting as an early warning system. In this context, the technology can highlight conditions that could potentially be suspect such as objects left in an area; cars parked where they should not be, or excessive densities of people in an area. This technology is starting to become more common with advanced DVR systems.

Potential Areas of Developments: Other technologies offer substantial potential, but have some development time still to go before they reach effective use. Where an operator is viewing a scene and needs to divert his or her attention to something else, parallel monitoring or tracking through tagging a particular object or person could allow operators to come back to that scene later and pick up more easily on the location and movement of the target.

Various ‘video analytics’ have found favors with the security professionals and many more are being developed. Psychological profiling thus will be easy in complex situations. Building up an information base on targets, situations, and behaviors to use for risk management and future investigation is one of the most neglected aspects of CCTV.

Intelligent Technology: Use of an intelligent system that recognizes behavior and conditions can greatly help by increasing the amount and quality of information coming in. Technology can also help by simulating or verifying operator performance, either in contrasting the number of issues picked up by the intelligent systems, or the insertion of scenarios that should be picked up by operators and reviewing them against actual detection scores.

Finally, intelligent technology can be used to extend the normal CCTV functions by building in algorithms that allow the detection of other things such as fire, smoke, production stoppages, overflows and so on that would add value to the CCTV function. I think the potential for intelligent analysis, sometimes called visual analytics technology, goes far beyond security-based CCTV to many forms of risk management and monitoring. The questions on “what, where, when, who, why and how” will increasingly become available in our data retrieval system.

Implementation Problems: Besides the development needs that are required to realize some of the ideas for technology, there are some implementation problems with those we already have available. Cry wolf is when repeated warnings occur without foundation. Eventually, the people start disregarding the warnings and the potential of the technology becomes ignored.

Use of blank screen-based alarm systems are a classic example, after 90 false alarms popping up on screen in an hour or two, the screens often get switched off because they are just seen as a distraction. We can also overload the operator with warnings on what could be happening so that they do not have the time to deal with everything they are faced with. Priority setting in such instances becomes important.

We do not want CCTV to be reactive to only technology-based detection - people are still more efficient at being proactive and picking up dynamics and behavior. If we prevent them searching for incidents, we will probably miss some of the most important. The timing of the event occurrence, or when we warn the operator is also something that needs to be considered. Too soon may just provide a lot of false alarms, too late may be exactly that - too late. Finally, where do we place the warnings within the display environment - does it become the centre of attention, or one of the tools the operator uses.

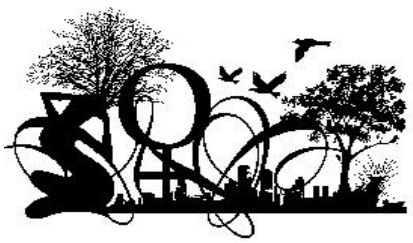
Envisaged Improvement in performance: Technology has the potential to deliver higher performance in a number of ways:

- ***The level of work being performed* -** people can concentrate on the important and higher priority issues that need human interpretation.

- ***The volume of coverage of the system* -** all of these cameras are really working - not just providing a mass of information that will largely be lost and discarded. Clients are getting real capital return on their system investment. Event generated alarms and video monitoring and tracking helps! Privacy ensuring blockage of pre-determined areas help greatly in avoiding litigations on breach-of-privacy related matters.

- ***The quality of results delivered:*** This is surely going to provide higher security related out-put: more things are being detected, and the base is being laid for a more intelligence and directed risk management process.

In five years' time, we will find intelligent systems on just about every worthwhile CCTV site. However, despite all the limitations with CCTV systems, the operator is still the key and final decision maker. The right operators make a significant difference to the system. Operators will continue to be able to do things that technology is unable to do and will do so for some years to come.



Traditionally women have always been considered the weaker sex and have been given a position below men. Times have changed and women have started getting at par jobs and positions with men. But they continue to be insecure in this society. The need of the hour is to empower the working women so that they need not be the downtrodden whom

anyone could take advantage of. Crimes against women are increasing by the day. Especially working women who have to commute between places as also spend most of the day in a male dominated workplace. Women are being cheated and harassed by women themselves.

An incident, which happened at Pallikkara in Kerala, is an example of how women themselves dupe their ilk for benefits. A household was robbed of money and jewellery by a group of women who posed to be rag pickers. Only an aged lady was present at the house and these women used a very simple technique to dupe her. A group of 4 to 5 women, they divided themselves in to two with one team approaching the old lady inquiring for old kitchen utensils and slowly moving to the rear of the house in the guise of checking for any rags that maybe there. The old lady who followed them inadvertently left the front door open and the second team coolly went inside and denuded the house of all valuables and vanished.

This happened in a house where the old lady's son and wife goes to work as also their children to school and she is left alone in the house during the day. This instance brings to right the need to educate our old people about the need to be careful about such attempts. The need to ensure the security of the old people whom they leave in their houses is very important.

A Correspondent had interviewed some of our lady employees to gather an insight into the difficulties they face due to the lack of security in this world. One of them has the opinion that the most literate state of the country offers no respects or security to their womenfolk. She has (had) the opportunity to serve in other states where people were not as educated, but they respected their womenfolk and were protective about them. The increase in sophistication and urbanizing has only resulted in increased lack of security for women. In her opinion the rural areas are more secure than the urban ones. Another lady had a different opinions and feels women are secure in this society and people tend to respect them, while one another says that she has never had to face a situation of insecurity in her life.

Whatever be the personal opinions or experiences of our womenfolk, it needs no emphasis that security should be given high priority be it at home or workplace or in society. Small tips can go a long way in ensuring the safety and security of our womenfolk and their family. It would be worthwhile to mention the time tested safety pin defense which has many a time proved very effective for women traveling by public transport. These days we have ladies training themselves in martial arts and other forms of defense techniques to protect them in the society. The need to hone ones skills to react correctly and effectively to a situation is very important and training in martial arts essentially aim at developing ones reaction capability.

Few tips that would be helpful-

- Whenever you travel or plan a journey do it in groups. Avoid individual travel as far as possible.
- Secure your homes when you leave behind aged people or children behind.
- Give them a phone, which they can easily operate in an emergency.
- Highlight emergency telephone numbers and ensure they are stored in the telephone, or are displayed in a prominent place.
- Provide a secure grill at all door that open outside, be it on the ground or higher floors. Ensure that the grills are closed and secured so that any attempted forced entry can be effectively aborted.

- Instruct your aged folks and children not to open the grill for any strangers.
- Screen servants before you employ them.
- Contact the people at home on phone at regular intervals.
- Do no make appointments with any repair/service agency while you are not at home.
- A little care can see you a long way.

Secure and non-secure web pages . . .

Important information

Courtesy: Col Arvind Singh, (arvindkanu@yahoo.com)

What is the difference between http and https?

Don't know how many of you are aware of this difference, but it is worth sending to every one....

The main difference between http:/// and https:// is it's all about keeping you secure! HTTP stands for Hyper Text Transfer Protocol.

The S (big surprise) stands for "Secure"…

If you visit a website or web page, and look at the address in the web browser, it will likely begin with the following: http:///.

This means that the website is talking to your browser using the regular 'unsecured language. In other words, it is possible for someone to "eavesdrop" on your computer's conversation with the website. If you fill out a form on the website, someone might see the information you send to that site.

This is why you never ever enter your credit card number in an http website! But if the web address begins with https:// that basically means your computer is talking to the website in a secure code that no one can eavesdrop on.

You understand why this is so important, right?
If a website ever asks you to enter your credit card information, you should automatically look to see if the web address begins with https://

If it doesn't, you should NEVER enter sensitive information.... such as a credit card number.

"The more you find out about the world, the more opportunities there are to laugh at it."

- Bill Nye

SOMEONE IS SPYING YOUR MOVES

How to detect a 2-way mirror?

Have you seen recent advertisement of M/S SAINT GOBAIN GLASSES shown in Televisions - Then you must have known about 2 Way mirror)

How to determine if a mirror is 2 way or not (Not a Joke!)?

Not to scare you, but to make sure that you aware. Many of the Hotels and Textile showrooms cheat the customers this way & watch privately.

HOW TO DETECT A 2-WAY MIRROR?

When we visit toilets, bathrooms, hotel rooms, changing rooms, etc; how many of us know for sure that the seemingly ordinary mirror hanging on the wall is a real mirror, or actually a 2-way mirror i.e., they can see you, but you can't see them. There have been many cases of people installing 2-way mirrors in female changing rooms or bathroom or bedrooms. It is very difficult to positively identify the surface by just looking at it. So, how do we determine with any amount of certainty what type of mirror we are looking at?

CONDUCT THIS SIMPLE TEST:

Place the tip of your fingernail against the reflective surface and if there is a GAP between your fingernail and the image of the nail, then it is a GENUINE mirror. However, if your fingernail DIRECTLY TOUCHES the image of your nail, then **BEWARE; IT IS A 2-WAY MIRROR!** (There is someone seeing you from the other side). So remember, every time you see a mirror, do the "fingernail test." It doesn't cost you anything. It is simple to do. This is a really good thing to do. The reason there is a gap on a real mirror, is because the silver is on the back of the mirror UNDER the glass. With a two-way mirror, the silver is on the surface. Keep it in mind! Make sure and check every time you enter in hotel rooms. May be someone is making a film on you.

Ladies: Share this with your friends.

Men: Share this with your sisters, wives, daughters, friends, colleagues, etc.

Security is when everything is settled…when nothing can happen to you!
Security is the denial of life!"

- Germaine Greer

Feedback:

Dear Mr. Tyagi,

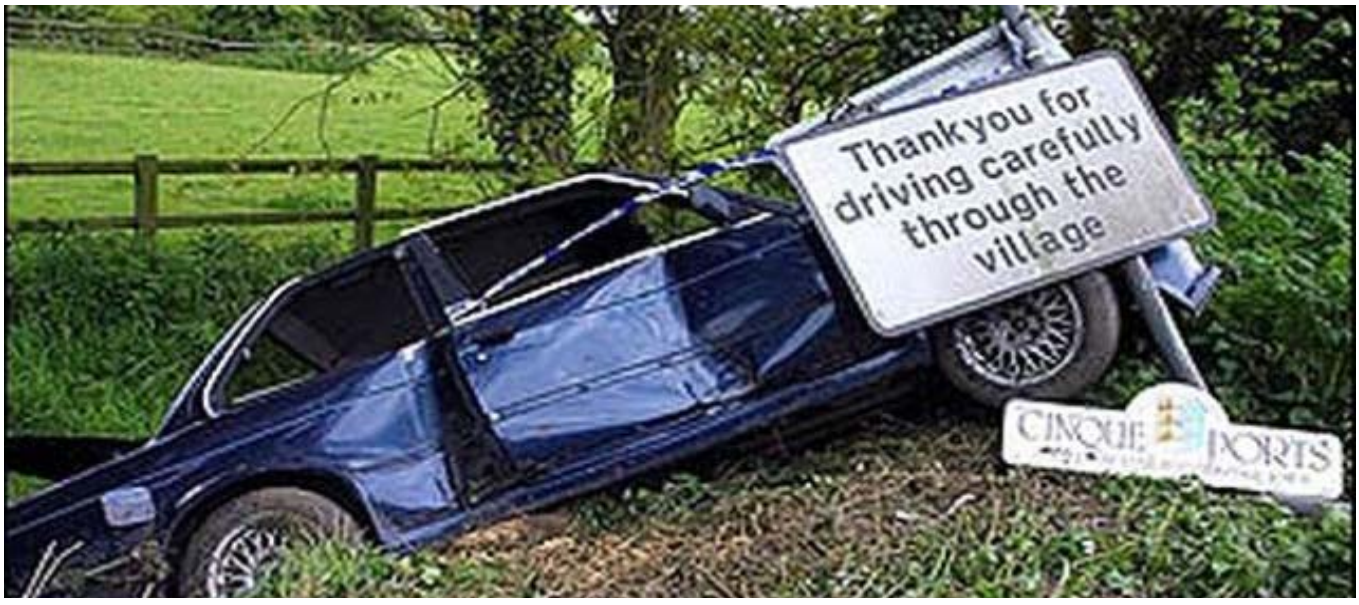
Thank you for the Newsletter. You have mentioned CISF strength as 1 million. I think it is about 1, 25,000 or so now and certainly not 10 lakhs i.e.1 million. Even all CPMFs together will not be one million. Similarly number of CISF units and airports is not correct and is not an updated figure. Airports guarded by CISF are about 54 or so, not 16. I am a former CISF officer. You may please see that there are some spelling mistakes, like 'sence' instead of 'sense'. You may please consider correction after going through CISF website/other sources…

With Regards
T V Ramana
VP-Tech Services
Raxa, GMR Group

Response:

Thank you Mr. Ramana for the response!
On CISF numbers, you are right and I was wrong! I assure you that spellings will be checked and re-checked. Your response indicated that newsletter did draw your time and attention. Your contributions in form of articles, news and photos will be highly appreciated.

Best regards
Capt SB Tyagi



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