# International Council For Industrial Security & Safety Management

## Newsletter: July 2013

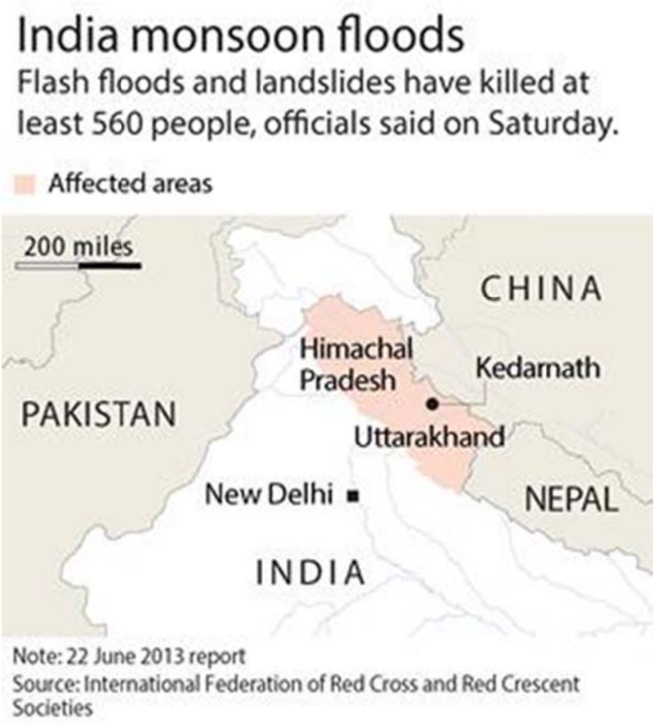
*Let's professionalize the professionals…*

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

## Uttarakhand Tragedy: Largest Helicopter Rescue Operation in the World

Sending a word of assurance, Indian Army Chief, Gen Bikram Singh on Friday, 28th June 2013 said the Armed Forces will continue their operations till all the people are rescued from various locations in flood-hit Uttarakhand. He had asked his commanders to launch relief operations in "very, very difficult conditions" in a proactive manner, without waiting for any requisition from authorities. "Our endeavor is to locate all our citizens, wherever they are, and get them out," he told reporters here. Gen Singh said he was visiting the area to laud the efforts of over 8,000 personnel of the Army, along with the troops of the ITBP, NDRF and IAF.

Many of the troops deployed in relief operations are from Garhwal Rifles unit, the Army chief said, adding that Garhwal Scouts are from Uttarakhand and their families were also impacted by the flash floods. "They are son of soils and large number of them are affected too. I must tell you these boys have refused to take leave to attend to their kith and kin and rather render their duties. We all had a phenomenal synergy," Singh said.

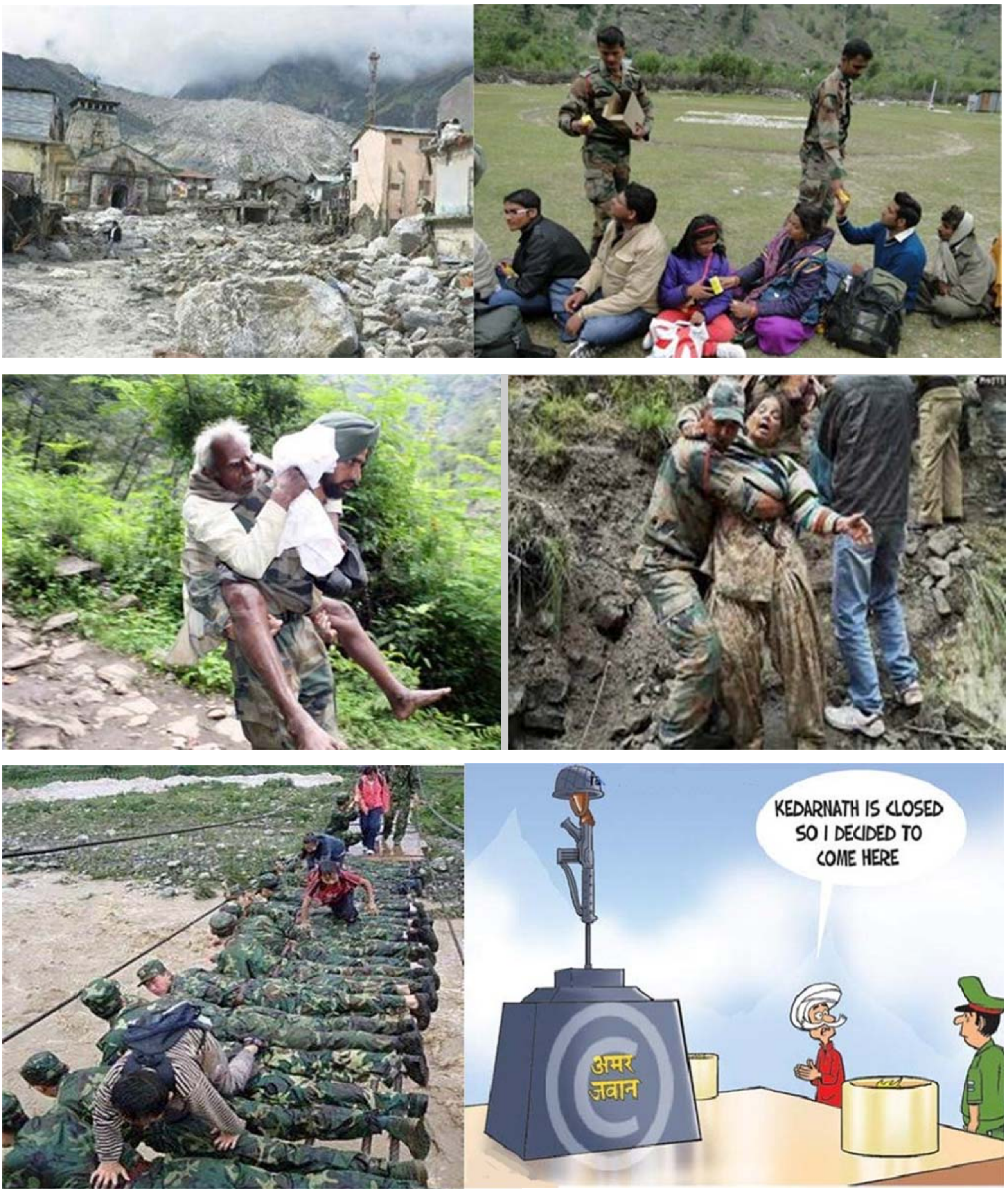

India monsoon floods

Flash floods and landslides have killed at least 560 people, officials said on Saturday.

Note: 22 June 2013 report

Source: International Federation of Red Cross and Red Crescent Societies

**This year's early monsoons caught hundreds of thousands of tourists, pilgrims and residents by surprise.**
**Soldiers recovered more bodies as they cleared debris in villages flattened by landslides and monsoon floods in the northern Indian state of Uttarakhand, bringing the death toll from torrential rains above 1,000, the Indian Home Minister said.**
**Army troops are attempting to rescue more than 10,000 stranded people, many in the temple town of Badrinath in Uttrakhand. More than 68,000 people have already been rescued.**
**The unprecedented heavy rains triggered landslides and floods in the Ganges River 17-18th June 12, washing away thousands of houses and roads and cutting communication links in large areas of Uttarakhand.**
**Uttarakhand is a popular summer vacation destination for tourists seeking to escape the torrid heat of the plains. It is also a religious pilgrimage site with four temple towns in the Garhwal Himalayan range. Most of the people stranded in Uttarakhand are Hindu pilgrims at the four revered shrines. The tourists usually return before monsoon rains begin in July. But this year, early rains caught hundreds of thousands of tourists, pilgrims and local residents by surprise.**



**We salute all the brave hearts involved in rescue operations who laid down their lives to save others'! We also offer prayers for ever lasting peace to departed souls and pray to God to give strength to bereaving family members to bear the loss!**

# Addressing National Concerns over SCADA Security

As the popularity of supervisory control and data acquisition (SCADA) systems continues to rise, companies across the globe are seeking how to effectively manage any changes within the organisation with seamless upgrades. Alongside optimising the SCADA system, firms need to ensure that threats to it are countered with advanced security measures – the importance of which was recently highlighted by a global attack by a worm known as Stuxnet.

The worm is a new form of security threat which represents a potential risk to critical infrastructure and has already made waves by affecting Iran's weapons programme and causing chaos by slowing down internal processes.

This worm was recently brought under the spotlight by Tom Parker, director of Security Consulting Services at security vendor Securicon, who attempted to uncover the risks it poses to SCADA and other control systems and how to defend against them. He analysed the code complexity of the virus, and told InternetNews.com:" One of the analysis mechanisms I've written looks for amateurish mistakes in code like heavily nested conditional statements. Typically, a more advanced programmer will be aware of efficiency issues in code and heavily nested statements is a fairly typical mistake among people that are just learning how to program."

However, he said Stuxnet also has some very advanced components and is not entirely uniform as there are at least four versions, two of which have significant differences. He noted that Stuxnet did not have many of the Microsoft vulnerabilities in it that later versions exploited, while one of the vulnerabilities was a link shortcut file issue. Mr Parker said that Stuxnet is a worm with its crosshairs "targeted" on SCADA control systems, particularly for infrastructure such as power plants.

"Control systems are designed around having the minimum required functionality - they're designed to be efficient and reliable. A lot of these systems are reliant on other infrastructure to protect them, and many don't even have password access as they've been operating in closed environments," he told. The expert noted that SCADA systems are not used to being exposed to the same types of threats that are common on the internet and it will therefore be some time until they can "stand alone" against modern attacks.

Organisations currently utilising SCADA systems are exploring how they can standardise security for these systems and protocols and establishing secure systems in an integrated environment, as well as implementing methods to counter security risks. With the rapid growth witnessed in supervisory control and data acquisition (SCADA) systems during recent times, organisations across the world are continually finding new ways to effectively manage change with seamless upgrades. But as well as optimising the SCADA system, firms crucially need to ensure that advanced security measures are in place to counter external threats with the potential to floor national infrastructure.

The urgency of this was highlighted last year by news of a high-profile global attack – at its centre was a worm by the name of Stuxnet. It infected tens of thousands of Windows PCs running Siemens SCADA systems in manufacturing and utilities organisations, most notably in Iran. Stuxnet proved that it is relatively simple to cause potentially catastrophic damage" to an industrial control network.

Industrial networks have evolved from humble beginnings at standalone plants, into the fully-distributed, integrated systems linked directly into businesses and responsible for monitoring and controlling today's national infrastructure. As technology has developed, sensors and actuators upgraded the basic manual interface, though it was the advent of microprocessors that led to the creation of sophisticated networks that service the industry to this day. But with the birth of new technologies, the potential for things to go wrong also seems to have been amplified somewhat.

Writing for PublicService.co.uk, the British Security Industry Association's (BSIA) David Ratcliffe, said recently that as systems became more complex, their security was rather lacking. "Everything was transmitted across the wire in clear text, as there was no real need for securing the data. After all, the idea of someone intercepting the data, altering some variables and causing the system to fail or crash was unthinkable, as these were installed in factories and pump halls and the protocols were obscure and proprietary, with no links to the outside world," he explained.

Influenced by work undertaken in the US, European governments began to recognise long ago that SCADA systems were potentially vulnerable to external threats. For example, the Centre for the Protection of National Infrastructure (CPNI) in the UK has issued directives urging companies to start making security a key priority. The CPNI is helping Britain's core infrastructure understand and mitigate electronic attack risks, facilitating these efforts through a focussed programme of work.

As the BSIA's Mr Ratcliffe pointed out, security is and will remain of paramount importance wherever industrial systems are concerned. Key to ensuring that requirements are met, government intervention will be needed continually, with thorough regulation and guidance in place to keep firms on the right track. "The increase in IT-type architecture for SCADA systems has given us an unhealthy confidence," he suggested.

Mr Ratcliffe continued: "Just like pirates in 2010 can hold ships off the coast of Somalia for millions of pounds in ransom, the idea of a power plant being disabled or taken over by a group of cybercriminals should not be considered absurd. Not only is there now a concerted effort to attack industrial networks by organised groups, but individuals now bored with creating simple email viruses are also looking for a new challenge. The virtual war that IT departments went through will eventually come towards our industrial networks."

The challenge for industry now is to keep investing in and securing its crucial networks, carrying them into the future with robust layers of ideally impenetrable layers of security. Vulnerabilities in SCADA systems may not be as headline-grabbing as other threats, such as those throughout e-commerce activity, for example, but the fact remains that an attack could be equally – if not significantly more – devastating than cybercriminals' interfering with the likes of PayPal and Amazon. Governments are increasingly recognising this, but so too are the attackers. And the battle to protect national infrastructure rages on.

# Aviation Security

Large numbers of people pass through airports every day, this presents potential targets for terrorism and other forms of crime because of the number of people located in a particular location.[2] Similarly, the high concentration of people on large airliners, the potential high death rate with attacks on aircraft, and the ability to use a hijacked airplane as a lethal weapon may provide an alluring target for terrorism, whether or not they succeed due their high profile nature following the various attacks and attempts around the globe in recent years.

Airport security attempts to prevent any threats or potentially dangerous situations from arising or entering the country. If airport security does succeed in this, then the chances of any dangerous situations, illegal items or threats entering into aircraft, country or airport are greatly reduced. As such, airport security serves several purposes: To protect the airport and country from any threatening events, to reassure the traveling public that they are safe and to protect the country and their people.

Security has been a matter of concern for civil aviation for several decades, but in particular since the bombing of a flight above Lockerbie in 1988. However, aviation security has, up until more recently, been addressed on essentially a national level. At the international level, though for some time Standards and Recommended Practices have been laid down by the International Civil Aviation Organization (ICAO) for States to implement, these are not regulated by a binding mechanism to guarantee their full and proper application.

Following the terrorist attacks in the United States on 11 September 2001 when commercial aircraft were used as weapons of mass destruction, the Commission made a legislative proposal to bring aviation security under the EU's regulatory umbrella. This initiative led to the adoption of framework Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security and thus provided the basis for allowing harmonization of aviation security rules across the European Union with binding effect. That regulatory framework has since been overhauled by a new framework, in full effect from 29 April 2010, as laid down by Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.

Rescinding the limitations on the carriage of small pocketknives on board aircraft was always going to be a challenge. Like so many other measures that the industry has introduced over the years, it is always easy to add security measures, yet far harder to take them away. The brouhaha that was initiated by the Transportation Security Administration's (TSA) recent announcement that knives with blades shorter than 6cms, of a width less than 1.27cms at their widest point, without locking or fixed blades and without moulded handgrips will, from 25 April, be permitted in carryon baggage was to be expected, especially in the United States in light of the fact that box cutters (which will remain banned) were used in the perpetration of the attacks on 11th September 2001.

The debate, which has become a huge political issue, emphasises three things. Firstly the problem with knee-jerk procedures being implemented as a response to a terrorist attack; secondly, the extent to which intelligent people fail to deploy common sense and allow their emotions to rule their decision-making processes; and thirdly, the frightening willingness of certain groups to hold onto politically acceptable security measures, such as the ban on knives, whilst rejecting effective, yet politically sensitive, security measures, such as profiling, whilst arguing the case that they are speaking on behalf of those who died in 2001.

Some incidents have been the result of travellers being permitted to carry either weapons or items that could be used as weapons on board aircraft so that they could hijack the plane. Travellers are screened by metal detectors. Explosive detection machines used include X-ray machines and explosives trace-detection portal machines (a.k.a. "puffer machines"). In the United States the TSA is working on new scanning machines that are still effective searching for objects that aren't allowed in the airplanes but that don't depict the passengers in a state of undress that some find embarrassing. Explosive detection machines can also be used for both carry on and checked baggage. These detect volatile compounds given off from explosives using gas chromatography.

A recent development is the controversial use of backscatter X-rays to detect hidden weapons and explosives on passengers. These devices, which use Compton scattering, require that the passenger stand close to a flat panel and produce a high resolution image. A technology released in Israel in early 2008 allows passengers to pass through metal detectors without removing their shoes, a process required as walk-though gate detectors are not reliable in detecting metal in shoes or on the lower body extremities. Alternately, the passengers step fully shoed onto a device which scans in under 1.2 seconds for objects as small as a razor blade. In some countries, specially trained individuals may engage passengers in a conversation to detect threats rather than solely relying on equipment to find threats.

Generally people are screened through airport security into areas where the exit gates to the aircraft are located. These areas are often called "secure", "sterile" and airside. Passengers are discharged from airliners into the sterile area so that they usually will not have to be re-screened if disembarking from a domestic flight; however they are still subject to search at any time. Airport food outlets have started using plastic glasses and utensils as opposed to glasses made out of glass and utensils made out of metal to reduce the usefulness of such items as weapons.

# Travel Tips

**A must read for anyone traveling by air! Following tips will help you reduce your wait time at the security checkpoint.**

- **Do NOT** pack or bring prohibited items to the airport.
- Refrain from carrying unverified gifts or presents in wrapped package. If the package alarms, screener will need to unwrap it to investigate the source of the alarm.
- **Shoes, clothing items and other accessories that contain metal** will alarm the metal detector. As a result the screener will require you to undergo further checks which may include pat down frisking.
- **Put all undeveloped films and cameras with film in your Cabin (carry-on) baggage.** Checked baggage screening equipment may damage undeveloped films.
- Carry-on baggage is limited to one carry-on bag plus one personal item. Personal items include laptops, purses, small backpacks, briefcases, or camera cases. Remember, 1+1.
- Place identification tags on all your baggage. **Don't forget to label your laptop computer.** These are one of the most forgotten items at Screening Checkpoints.
- Refrain from packing valuable items in your checked baggage (Regd. Baggage). Once you hand your baggage to your air carrier, security staff of the air carrier will handle and process the baggage in the prescribed manner Please keep in mind that most air carriers have limited liability for lost, damaged, or stolen items.
- Declare fire arms and ammunition to your airline and place it in your checked / registered baggage.
- Protect yourself and do not pack valuables in your checked baggage.

**Your Cabin / Carry-on Baggage**

- Carry all metal items in your carry-on bag. This includes jewellery, loose change, keys, mobile phones, pagers, and personal data assistants (PDAs).
- Take your laptop and video camera out of their case and place in the tray provided at the security checkpoint.
- Place your overcoat or jacket in the tray at the security screening Checkpoint. Suit jackets and blazers need not be removed, unless requested by the screener.
- **Do not leave your baggage unattended**
- **Do not accept baggage from strangers.** It may contain prohibited items or dangerous goods.

## Travel Safe and Smart

**Preparations**
Necessary preparations can be made by you before arrival at the airport which will help you to move more quickly and efficiently through the security processes. Here you will find suggestions on what to wear to the airport and how to pack for your trip. We've also included a pre-flight checklist to help you to travel safe & smart.

- **Dress**

Security does not require any particular style or type of clothing. However, certain clothing and accessories can set off an alarm on the metal detector and may affect the pax flow through the screening points. **Here you will find tips to help you**

- **Pack Smart**

There are restrictions on what you can pack in your hand baggage and registered baggage. All of your baggage will be screened and possibly hand-searched as part of the security measures. This inspection may include emptying most or all of the articles in your bag. **Here you will find tips to help you pack.**

- **Final Checklist**

You're dressed, packed and ready to go. **Here is a pre-flight checklist to help you to travel safe and smart.** Read the instructions printed on the air ticket and contact your airline or travel agent for additional information.

- **Access Requirements**

You can enter into the passenger terminal if you have either a confirmed air ticket for the journey or a valid airport entry permit. Visitors can buy ticket to enter into the visitor' s area in the terminal. Waitlisted passengers are advised to contact the airlines office on the landside of the terminal for confirmation of their tickets.

- **Security Process and Procedures**

Familiarise yourself with the Security Process and Procedures. It will help you to play an active role in ensuring your own safety and avoid inconvenience to yourself.

# How Fraudsters are working in Our Country to Cheat Innocent Citizens?

**Col N N Bhatia (Retd)**
**Industrial Security Consultant**

On 30 May 2013 around 1115 hrs. I got mobile call from my son - Capt Gaurav Bhatia (Mob No 0994046xxxx), who has joined new company in Chennai on 3 May 2013, stating that one person who said he was Sub Inspector Rana from the Special Branch (Crime) Delhi Police rang him from Mob. No. 08800879719. He told him that there was a case against him (Capt Gaurav Bhatia) under IPC Sections 406, 420, 468 and so on. My son asked him what crime he had done, who has lodged the complaint and how he got his new Chennai number given to him by his company only a few days back? Mr. Rana said he (Gaurav Bhatia) had cheated RBI and for more details he should contact Mr. Narinder Kumar, Government Lawyer at Patiala House immediately as he (Gaurav Bhatia) was to be present in the court at 1150 hrs. on 30 May 2013 failing which non-bail able arrest warrant would be issued against him and sent to Chennai Police. Once he was arrested his passport etc. would be cancelled and he would lose his job too.

My son, quite worried, rang me immediately and appraised me what has been stated in Para one above and SMSed me Mr. Rana's mobile No. I was very upset and rang Mr. Rana immediately and asked him the details of the case. He said Gaurav Bhatia was required to be present in Patiala House Court at 1150 hrs. on 30 May 2013 in cheating case reported by the RBI failing which non-bailable warrant of arrest would be issued against him and sent to Chennai Police for his arrest. I asked him that there was a procedure on recovery of dues by government and no notice or letter to this effect has ever been received by Gaurav Bhatia or any one of us. He told me that since the case file was 12-13 pages long, he could not read and tell me the details and that I should contact Narinder Kumar (Mob No 09540263218), Government Lawyer dealing with the case. He also warned me repeatedly that required action should be taken by me in next 10 minutes after talking with Narinder Kumar and I must tell him before 1150 hrs. or else he would issue non-bail-able arrest warrant against Gaurav Bhatia.

After repeated ringing, I was finally through to I Mr. Narinder Kumar who initially said he could not recollect the case and I should ring him after 5-10 minutes. In between I got again call from Rana wanting to know if Narinder Kumar has issued 'hold' order on the case. I again rang Narinder Kumar and he said RBI has filed a case against Gaurav Bhatia as he has not paid the bank Rs 76200.00 dues since long. I desired to meet him in Patiala House & he said he was very busy & I should meet him around 4 pm. I asked him his chamber /office location & he said I should come to Gate No 2 and ask anyone for him. When I told him that Mr. Rana had said that the deadline was 1150 hrs. on 30 May, he replied in that case, I should rush to nearest ICICI Bank with a cheque book and contact him and he would give the account number in which the money was to be deposited. I told him what details I need to fill in the challan & he said I should better rush to the bank first & ring him from there. Mr. Sudhir Walia, Senior Lawyer of the Supreme Court who lives in Noida, is

The author is army veteran having more than three decades of colourful service in various command and staff functions. He also had a very long and mentionable tenure with Intelligence Bureau where he was associated in inspection and audits of industrial security measures undertaken by PSU and government establishments.

An avid reader and prolific writer, Col Bhatia is now freelance consultant in the field of Industrial Security & Safety Management. He is passionately involved in efforts for release of Indian POWs held in Pakistan. He can be reached by e-mail at - narindra_bhatia@hotmail.com

my relative and was away to Chandigarh, I rang him for consultation and gave him Mobile numbers of both Mr. Rana & Mr. Narinder Kumar. Soon after Mr. Rana again rang me and asked me what actions I had taken. I told him I was a former Intelligence Bureau Officer, I would contact my former 'IB Bosses' and would act on what they and Mr. Walia would advise me. He said, *'phir, mein apni kaarrya wahi shuru karta hun'* or words to that effect and hanged up.

Meanwhile, Mr. Walia told me that it appears to be well organised syndicate working as he got it checked from the Patiala House Courts and no case RBI versus Gaurav Bhatia was listed for hearing on 30 May 2013. He also got it checked that there were 5 lawyers registered in the Patiala by the name Narinder Kumar and none of them had Mobile number as 09540263218. Mr. Walia also rang number of times to Rana and Narinder Kumar. While Mr. Rana never lifted the mobile, Mr. Narinder Kumar once lifted the phone and when Mr. Walia told him he was his professional colleague practicing in Supreme Court he fumbled answering Mr. Walia's queries and left the phone. Thereafter, there is no communication with both Mr. Rana and Mr. Narinder Kumar. Whole incident has put us in avoidable tension and appears to be part of organised cyber / white collar / financial crimes that need to be investigated and criminals punished. Since I had served in the Intelligence Bureau for over 8 years after retiring from the Army, I contacted some of my retired senior colleagues. The analysis of mobile numbers of Rana and Kumar are fake and from area around Ghaziabad. The case may be referred to Special Branch Delhi Police for further investigation and to catch the culprits.

A piece of advice-please ensure you and your family, specially the children on Facebook do not give personal details like mobile numbers, residential /official addresses, family details, bank account numbers, car numbers etc. so that the unscrupulous elements do not misuse them.

---

# Feedback:

**Anirudha Singh** <anirudhsingh@rsecurity.in>

Date: 8.06.2013

Dear Sir,

Thanks for News Letter. I have gone through the important articles. About the incident which took place on 20th Feb in Noida during trade union strike, I should say that the culprits must be identified and punished, concerned trade unions must be penalized. Workers have not put the property of owner on fire, but they have put their own property on fire. Factories are the means of their livelihood and they support their family by earning from it.

On 21st Feb 2013, when Bharat band was going on, one shocking incident occurred in Ranchi. Three employees of an industrialist, had kidnapped the owner on 14th Feb 13, and his dead body was recovered on 21st in a jungle. They had killed brutally 70 years old industrialist Mr. Gyanchand Jain and buried in jungle near Ranchi. The conspirator was his driver Mukesh, who was once removed from service due to dereliction on duty. He apologized and had rejoined the service few months ago. The whole business world in Ranchi and Jharkhand was in turmoil and had called another bund on 22nd Feb, too.

The above two incidents compel us to rethink about the philosophy of industrial relations, owner-worker relations and role of Govt. There is need to redefine the doctrine of socialism, capitalism and Marxism.

Thanks & Regards,

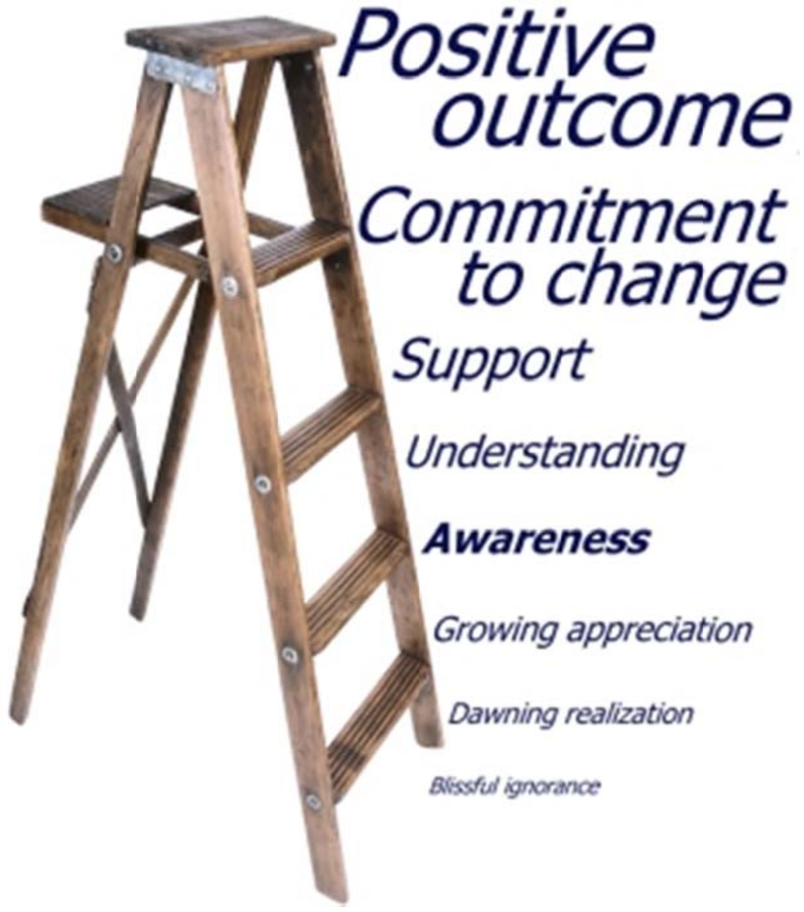
***Anirudha Singh, Director***

# Epilogue: Security Awareness

**Ira Winkler, a top security professional), wrote that "awareness mitigates non-technical issues that technology can't...you will find that security awareness is one of the most reliable security measures available." (Winkler, 2012)**

Your employees are your biggest security challenge. Constant education of users is crucial. When they join the company, a proper orientation should be held to explain the importance of information security, what it entails, what they should and should not be doing.

*Jack Loo*


Positive outcome
Commitment to change
Support
Understanding
Awareness
Growing appreciation
Dawning realization
Blissful ignorance