International Council of Industrial Security & Safety Management

http://onlineicissm.wixsite.com/iciss Newsletter: July 2017

Dear Security & Safety Professionals,

One noted security professional who works for a major refinery once pointed out, “our industry is one such that a loss of access or control over our systems usually means someone dies”. Regardless of the potential harm, any industry with little or no security in and around their control system will at least lose production for some time. This can translate into re-work, overtime, environmental release, and other intangibles such as competitive edge, investor confidence and potentially the ability to stay in business.

The new push for control systems is to try to balance the two opposing trends: Access and Security & Safety. And the pressure is coming from many angles. Increasing market competition means that most industries are ‘pushing the envelope’ to run faster, more efficiently and with less downtime.

The scope of the term ‘security’ and 'safety' often seems vague and the sheer volume of effort and areas of concern this may represent can be overwhelming. However, this need not be the case. In looking at a number of security frameworks or standards a common theme emerges that is quickly being adopted as a holistic and effective approach to security.

The basic premise is quite simply that security and safety is important to the organization. This means the decision makers, the owners and operators of the systems, the support staff, the consultants, vendors, site staff, in short everyone, understands that keeping your facility safe and secure is in everyone’s best interest. This is no different from the importance placed on other business functions.

Try hard in your endeavors so that the decision makers in your organizations will take you as profit-center and integral part of the productivity and profitability.

Best regards

SB Tyagi
For ICISS

In this issue:

Un-Islamic State: Is World Ready for Solutions?

The ISIS have killed 22 persons in the UK last month.

We all know the ISIS have been scourge to human civilization. If there's a war crime to be committed, it appears ISIS is more than willing to carry it out. And, that includes indoctrinating young children and making them witnesses and accomplices to some of the militant group's most gruesome acts.

They have been routed out from their capital Raqqa. They have dug-in their heels in a small part of Syria. The ISIS have clearly been retreading, but they are still trying various methods to keep their forces ready. The attack in the UK has shown the ISIS have not been completely finished. This scourge to humanity has to be tackled by all countries.

World powers will have to face the civilizational challenge in combating the kind of terrorism that is being continued by the ISIS .The recent ISIS attack in the UK has to be controlled by world powers to save the world, no matter whether India, as a whole, and the Indian Muslims in particular, do not want to join the fight.

The 'Gazba-e-Hind' - the last crusade in India has been announced. The IS jihadis on the run from Iraq and Syria are finding safe heavens in Pakistan and Afghanistan. Bangladesh is their own country with umbilical connection!

The neighborhood all along India is very encouraging to the concept of Khurasan, establishing of which will form the firm foundation of world dominance of Islam -

We would rather emphasize that all concerned will have to fight the ISIS. That it has to be killed to the finish, must be the duty of all countries, small of big! Necessary means and preparations will have to be devised.

Islamic fundamentalists including the leaders of Al-Qaeda seized upon the legend of Greater Khurasan to inspire followers to pursue their terrorist agenda. According to legend Prophet Mohammed had prophesied that one day a great power would rise in the east to demolish enemies and spread Islam across the world. That created the legend of Greater Khurasan.

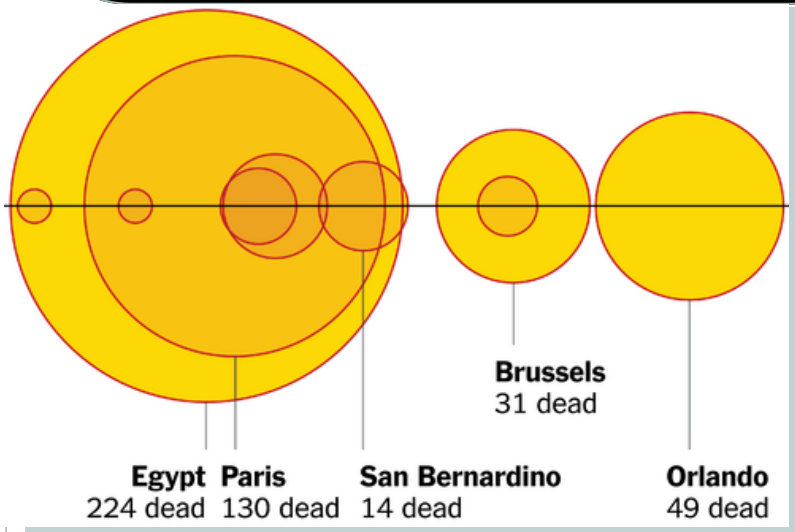
The traditional concept of Greater Khurasan included territories of Pakistan, Afghanistan and parts of Uzbekistan, Tajikistan and Iran as well as India. Well, it seems that the legend of Greater Khurasan is being overtaken by the reality of lesser Khurasan. And that might signify a crucial and much desired development.

The Islamic State jihadist group announced in 2015 that it has established a province in Khurasan. Abu Muhammad al-Adnani, identified as an Islamic State (ISIS, ISIL, or IS) spokesman, made the announcement in an audiotaped speech posted on jihadi forums.

Al Qaeda wants not the territory but an end to the United States' global hegemony. We have seen some experts making the mistake that Al Qaeda's dream of the Islamic Caliphate has been snatched by the ISIS, now the simple "The Islamic State".

In fact they are all the same, whether the Islamic State here or Al Qaeda there or the Islamic Brotherhood or the Boko Haram, etc in Africa!

Un-Islamic State: Is World Ready for Solutions?



A recently-leaked intelligence report claims that the Taliban and other regional players like Al Qaeda will be back in the saddle by 2017 as US winds down years more than a decade of military operations in the country.

One report suggests that ISIS cells in US & Europe are ready to launch Third World War. Islamic State has been calling in recruits from all across the globe – and it's not just men who answer. Young women come to IS to join the jihad, to be sex slaves for terrorists – or to commit terror attacks themselves. What lures girls into a life of fanaticism and violence? And how does desperation drive one into donning a belt with explosives? (https://www.rt.com/shows/sophieco/314326-isis-sex-slaves-terrorists/).

The big powers, which had formally called off the "war on terror" and started addressing the Islamic insurgents as only extremists, have not yet appeared in the scene effectively - may be because of the lessons learnt in Afghanistan or Iraq. Some are also busy in managing their home turf, having an ostrich-eye view all these years.

IS Threats Emanating in Europe:

- The scale and impact of "lone actor" attacks is increasing.
- A "real and imminent danger" is the possibility of elements of the Sunni Muslim Syrian refugee diaspora becoming vulnerable to radicalization once in Europe and being specifically targeted by Islamic extremist recruiters.
- Automatic firearms remain the weapons of choice of terrorist cells - but it is also possible that IS will consider the use of chemical or biological weapons in the EU, while car bombs could also emerge as an attack method.
- Counter-terrorism experts are concerned that Libya could develop into a "second springboard" for ISIS, after Syria, for attacks in the EU and the North African region.
- Individuals and groups involved in terrorist and extremist activities use encryption to conceal their communications from law enforcement and intelligence agencies

But, the situation unfolding here now, with the Islamic State having called upon all Muslims to join them, is too close to India, with Gujarat being specifically included in their scheme, to ignore its full significance and ramifications We do hope security strategists, both in the government and outside, are breaking their heads over this.

Perhaps, there is need for another prophet to emerge! Or, will the "true believers" continue to prove their nuisance for a longer period of time? Whatever be their ability, they cannot ultimately prevail. We must believe In That! The seriousness of the situation has to be taken to the members of the public, not only in the cities but to the rural areas as well. Sad to say but it is true more patriots are found in villages than among educated elites and so-called intellectuals.

In any case and on the whole, public opinion has to be built up to remain on the look-out for already identified/banned or not, outfits, spies and fifth columnists in all walks of life as also the "sleeper cells" suddenly becoming active.

Manchester must not be forgotten...

Cyber Security: Threat, Vulnerabilities and Solutions

Cyber environment is not safe…

Here no barbed wire...no dog barks...no patrolling...cannot hear the victim's scream…!

An assumption of fire wall and other measures misleads...there is a chink...as a layman with intuitive strength can understand...we are living and operating in cyber world with vulnerabilities…

All our critical sectors may it be defense, power, communication and others are susceptible to various threats...may it be hacking, virus, malicious malware (Trojan horse) unsolicited e-mails etc…

The writings in the book "Attacked, Hacked & Bombed" by Peter Lily gives an insight as to how our cyber environment is so vulnerable. We have not yet evolved a system in full strength to deal with this threat. Many of us do not understand the software technology and any explanation in technical language is like a dead foreign language. And all those at the gateway of the system are certainly not so equipped well to gauge the threat from Cyber.

In borderless environment of cyberspace, it becomes much more difficult to catch the cyber-criminals. In the absence of international pacts and treaties many criminals get away. More so attack of huge magnitude are being state sponsored. Our regulatory mechanisms at national as well international level are at infancy stage.

Many significant events suggest that we are not well equipped to contain the menaces in the cyber space.

The WannaCry cyber attack, which infected more than 220,000 computers in a single day in May, was the first incident announcing a frightening new trend – the marriage of ransom-ware and worms, spreading both through phishing attacks, and autonomously through networks. This time, most people were saved by a lucky coincidence that triggered a kill switch, but the next time, we won't be so lucky. Therefore, your information security needs a fresh approach, and the best option is to start with ISO 27001, the leading international standard for cyber-security.

As per information available in Media and various Cyber Security Forums, a massive Cyber-attack using Petya ransom-ware has major disruptions across various countries. It encrypts MFT(Master File Tree Table) of computer and show a ransom note and prevent victims from booting their computer until they pay a ransom. Such ransom-ware spreads through email having malicious attachment.

In view of the above, following Do's and Don'ts are advised:

DO'S	DON'T
Take regular backup of your files.	DO NOT OPEN the emails received from unknown senders and delete the same.
Make sure your PC antivirus is up-to-date. If not immediately, inform the concerned local BIS officer for taking necessary action.	If by mistake, email received from unknown sender is opened, then please DO NOT CLICK/ OPEN THE ATTACHMENTS to avoid encryption/ stealing of your valuable data.

Threats of Terrorism Targeting Oil and Gas Industries

'Energy security is among the most serious security and economic challenges, both today and in the future. As the economies of the World grow and societies develop, so does the importance of energy. And so does the importance of the infrastructures that produce and supply this energy'. This brings Oil & Gas Sector under sharp focus!

Human body charged with wickedness in brain is the most lethal primary weapon. All others are merely tools of terrorism.

Terrorist organizations have always been interested in targeting oil and gas facilities. Striking pipelines, tankers, refineries and oil fields accomplishes two desired goals: undermining the internal stability of the regimes they are fighting, and economically weakening foreign powers with vested interests in their region. In the past decade alone, there have been scores of attacks against oil targets primarily in the Middle East, Africa and Latin America. These attacks have never received much attention and have been treated as part of the 'industry's risk.'

As long ago as 2004 an Al Qaeda manifesto set out "laws" of targeting petroleum-related interests, pertaining to the "economic Jihad" with one of the primary targets being pipelines and supporting facilities and especially industry personnel "the easiest targets to attack and offer the greatest reward". The threats from terrorism to energy critical infrastructure exist for all to see, if they are willing to see that is, and that these so-call wicked risks are not going to diminish any time soon.

Today, a growing number of interconnected and diverse threats, mainly physical and cyber threats are challenging critical infrastructures. In that regard, terrorist threat is not a new phenomenon and critical infrastructures have long been attractive targets for terrorist groups and malicious acts. Especially, as being one of the most vulnerable sectors, Critical Energy Infrastructures have been subjected to increasing terrorist threat which is correlated with the growing political and economic instability in oil and gas producing regions. Furthermore, despite its enormous economic and political consequences, unlike other types of terrorism, energy terrorism could not attract a significant level of attention.

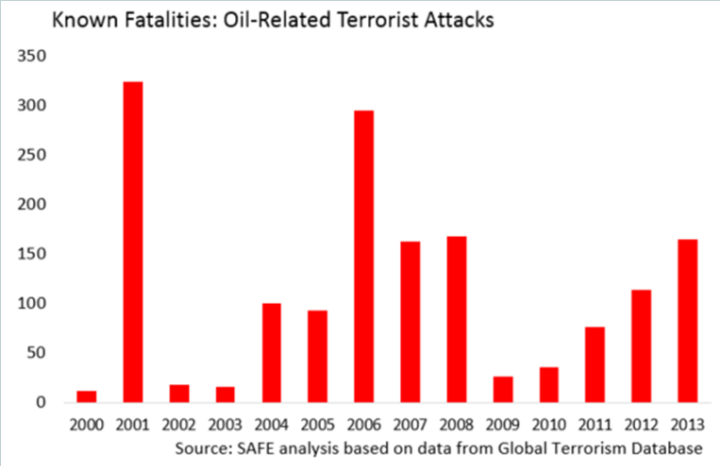
According to the University of Maryland's Global Terrorism Database, terrorist threats targeting oil and gas sectors have risen sharply. More precisely, during the mid-1990's, attacks on oil and installations reflected less than 2.5 of all attacks whereas in 2013, 600 out of 2600 total terror attacks targeted oil and gas sectors. (1) In fact, a wide majority of attacks concentrates in the Middle East and North Africa. However, from U.S to China, energy infrastructures are facing a varying level of threat (from theft to sabotage) which means that energy facilities worldwide have common vulnerabilities including inadequate controls at the borders; lack of a holistic security approach; lack of technology and lack of dedicated security

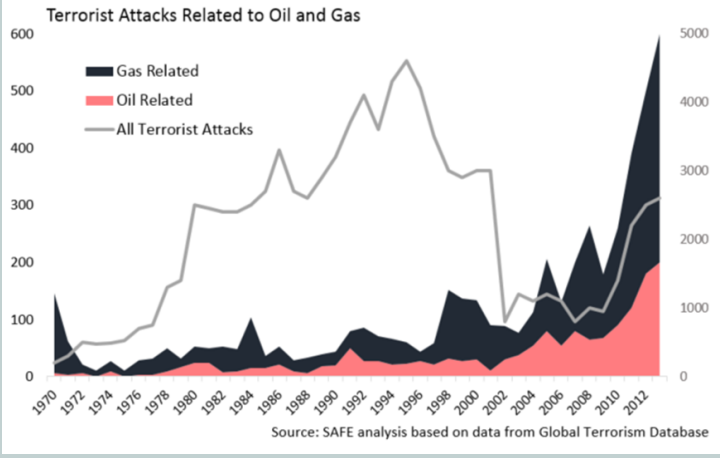
Oil & Gas Security Market

It is estimated to be growing from USD 26.34 Billion in 2015 to USD 33.90 Billion by 2020 at an estimated compound Annual Growth Rate (CAGR) of 5.2% from 2015 to 2020. These figures are according to 'MarketsandMarkets Researchers' in their recently published report entitled, "The Oil & Gas Security and Services Market by Application (Exploration & Drilling, Refining & Storage, and Transportation & Distribution). Oil & Gas Security is defined as the security process in which the oil and gas operational sectors namely upstream and downstream are secured with the help of stringent physical and the network security measures to ensure operational efficiency and minimize the losses associated with the security breaches. Researchers find that major forces driving this market is growing governmental pressure and security compliance and regulations, threat of terrorists attack and cyber-attacks and lack of comprehensive solution for oil and gas security and physical attacks and cyber threats.

forces etc.

Examining this trend more closely it can be seen that in 2003 roughly 25% of terrorist attacks were aimed at the energy sector, having jumped to 30% and 35% between 2003 and 2007 –the long-term trend revealing more attacks aimed at energy infrastructure (EI) occurring annually–. With oil accounting for nearly '40% of the world's energy and 96% of its transportation', the protection of energy infrastructure has thus become a top priority for most industrialized nations.





Threats over the Sea

There is growing evidence that terrorists find the un-policed sea to be their preferred domain of operation. Today, over 60% of the world's oil is shipped on 3,500 tankers through a small number of 'chokepoints' – straits and channels narrow enough to be blocked, and vulnerable to piracy and terrorism. The most important chokepoints are the Strait of Hormuz, through which 13 million barrels of oil are moved daily, Bab el-Mandab, which connects the Red Sea to the Gulf of Aden and the Arabian Sea, and the Strait of Malacca, between Indonesia and Malaysia. Thirty percent of the world's trade and 80% of Japan's crude oil passes through the latter, including half of all sea shipments of oil bound for East Asia and two-thirds of global liquefied natural gas shipments.

Pipeline sabotage is terrorist's weapon of choice

Until recently, the pipeline industry has been preoccupied primarily with environmental, safety and maintenance issues. Beyond occasional cases of vandalism, the human factor was hardly perceived as a threat to the world's vast web of oil and gas pipelines, which, all told, carry roughly half of the world's oil and most of its natural gas.

Pipelines, through which about 40% of world's oil flows, are another Achilles heel! They run over thousands of miles and across some of the most volatile areas in the world. Pipelines are also very easily sabotaged. A simple explosive device can put a critical section of pipeline out of operation for weeks. This is why pipeline sabotage has become the weapon of choice of the insurgents in Iraq. An attack on major oil installation, a chokepoint or a pipeline hub would be detrimental to any country's economy and likely to affect every aspect of lives of its citizens.

Petrochemical complexes and Oil installations on the hand are highly critical, highly vulnerable and sabotage and terrorist attack is highly

provable. This makes them also very attractive target with high "Terror Quotient" as damages here are likely to the lives and economy! The new breed of terrorists inspired or encouraged by ISIS will have knowledge of oil and gas installations operation and maintenance details and also would understand the vulnerabilities. Thus with more informed new breed of terrorists, world will see the renewed threats to this sector.

Challenges to Effective Security: Local Approach to Global Problem

Porous borders allowing terrorists from neighboring unstable countries to get through undetected to carry out such attacks on critical infrastructure;

Lack of a layered security approach and perimeters to prevent unauthorized access to critical facilities;

Lack of technology to provide early warning and detection of threats – both cyber and physical;

Lack of tools to provide a coordinated response to cyber-physical threats;

Lack of dedicated security forces to protect critical infrastructure in volatile regions of the world. There is much that needs to be done to change the way security is perceived and practiced by critical infrastructure owners and operators around the world.

Pipeline companies use advanced technology to monitor their infrastructure and keep a close eye for any leaks. For instance, Calgary-based TransCanada spent more than $1.5 billion on preventive maintenance programs in 2015, which included more than 700 digs to check pipeline integrity. Drones, pressure sensors and even specially trained dogs are used by industry to inspect pipelines, while other techniques are being developed.

"It is not enough," said Thiago Valentin de Oliveira, an electrical and computer-engineering master's student working on the project. "There is a major reason why — all of those monitoring systems that have been proposed in literature, they only detect leakage after it has happened. Our technology not only detects a leak, but also prevents it from happening. That is more important than anything."

Security Threat Mitigation Philosophy

The only effective counter is through a Joint approach, incorporating whole of government and the energy operating companies.

An approach that is at once –

- pro-active and robust (has authority and acts),
- builds resilience and recovery into its plans,
- is coordinated,
- Cooperates - in that both parties come out of their respective siloes and cultivate a Need-to-Share mind-set to information, and

intelligence rather than the traditional Need-to-Know model; and

- allocates the necessary funding, training and resources (dedicated specialist response force) to be effective at deterring, detecting and delay.

Security Solutions

- The existing passive model of risk management, normally utilised by the industry to mitigate safety, criminal, or environmental risks through weighing probability and impact is of little use in

predicting wicked risks, whose probability cannot be assessed (not quantifiable or insufficient statistical data) and whose impact can be catastrophic and far reaching both economically and socially. Typically, these risks have the characteristics of being unexpected and did not feature on risk assessments and planning; they were different than anticipated; were unpredictable in location, scope and impact; and can overwhelm the capacity to respond and deal with it immediately. The only effective counter is through a joint approach, incorporating whole-of-government and the energy operating companies.

With the threat of terrorism looming, pipeline operators in the industrialized world have taken action to prevent terrorism from harming energy infrastructure with steps that include:

- Increasing system redundancy,
- Deploying state-of-the-art surveillance equipment,
- Deploying aerial and ground patrols, and
- Fortifying pipeline systems against cyber-security breaches. Conducting periodic risk assessments to measure the level of risk and threat exposure to business operations;
- Addressing porous border issues to prevent terrorist movements across borders – especially in volatile regions;
- Expanding and securing the perimeters of critical sites to allow a multi-layered early detection, warning, deterrence and delay based solution to identify and deal with threats and adopting the use of advanced technology (sensors – manned and unmanned etc.) for early detection of threats, and securing pipelines.
- Companies also need to address the security gaps that evolve due to convergence of cyber physical threats – by adopting advanced cyber physical unified threat management solutions;
- Creating a dedicated critical infrastructure security force to deter and counter such attacks against critical infrastructure in volatile regions and countries.

'Lessons learned from accidents and safety incidents have been regrettable but they are critical contributions to instil safety in the DNA and operating culture of any prudent oil and gas operator.' In other words, it could be said that in order to implement and exercise best security practices for the energy industry, lessons learned from previous incidents should be well understood.

Numbers of best practices could be recommended for the Oil & Gas Sector -

- 'Security' should be considered and studied as an independent and distinct discipline from 'Safety' and it should be defined with clear objectives.
- Establishing proper mechanisms for 'Intelligence' and 'Information Sharing' is critical for assessing terrorism risks for a critical infrastructure. For instance, in order to eliminate insider threat and reach deeper information about their employees, companies could cooperate with state agencies in information sharing.
- A holistic and integrated security approach seems as a must in implementing corporate security policies.

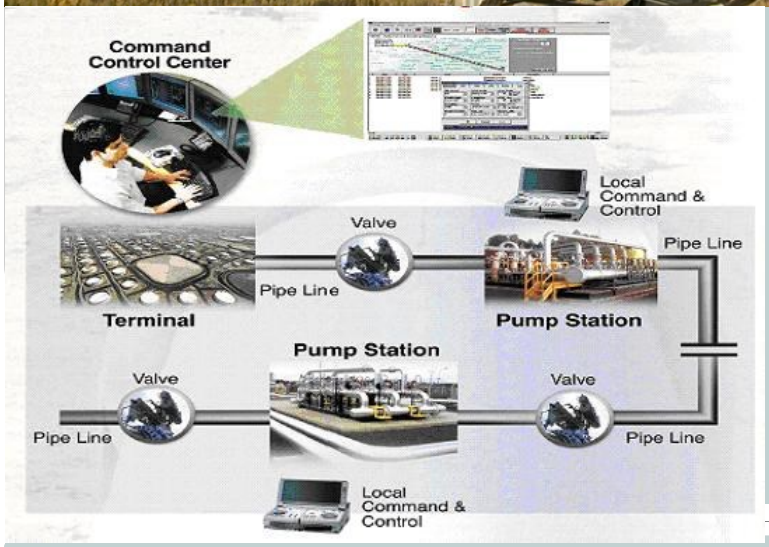
Developing alternative 'threat scenarios' with various inputs and outputs is an essential part

for a company's security plans. In other words, security departments should be capable to answer 'what if' questions regarding the changing conjuncture and threat and risk levels.

Conclusion

Terrorist attacks carried out by radical Islamist groups within the EU's borders are a concern and measures to prevent future catastrophic attacks must continue. However, as North Africa becomes a more significant supplier of energy to Western Europe, threats to the energy infrastructure in the region must also be considered.

Attacks or threats against energy infrastructures can lead to uncertainty amongst market players and overall insecurity, thereby raising global energy costs and placing additional budgetary pressures on states and consumers. To counter this trend and the inflexibility of the current energy environment, states need to adopt a multifaceted approach.



Forthcoming Events

GLOBAL DIGITAL SECURITY FORUM INDIA

Security Best Practices, Technology and Applications

31 Aug – 1 Sep 2017

Shangri-La Hotel, Bengaluru

Event Partner

What ICISSM is All About?

ICISS is purely non-commercial forum for security and safety professionals world-wide! It neither is with any support from any business groups nor is it projected by any business house in the background.

All its members have no stake in any solution providing or consultancy firms. Their association with ICISS is totally based on mutual benefit of knowledge sharing and networking.

We welcome all the security and safety professional world over from diverse background and encourage them to interact freely by asking the questions, replying them or by sharing their knowledge and experience.

The council also strives to have strategic alliances with similar forums world over for furtherance of its objectives.

Formed in 2010, the Council is totally apartisan, apolitical and does not represent any pressure group or interest group.

ICISS strives not to provide surrogate platform for anyone to enhance their respective business interest. It is thus totally professionals' body aimed at, 'professionalizing the professionals'!

We in ICISS believe that having different view than the majority is not bad! In fact we encourage difference of opinion and take every different views as intellectual stimulus to either convince or get convinced – either way both the parties are benefitted! Those who dare to think differently have shown that firstly they can think and secondly they are not overawed by the majority views! Such are the traits of 'Thought Leaders' and they deserve our respect!

For more details on our activities, please visit us at -

http://onlineicissm.wix.com/iciss

What ICISSM can do for you?

Consultancy: International Council of Security and Safety Management (ICISS) would be happy in providing consultancy to Corporates on all matters relating to Industrial Security Management from the best security professionals as it has on its panel the very best security professionals from almost all over the world. We have accredited security consultants from India, South Africa, UK, USA, UAE, Belgium, Libya, Yamane and Austria to name few countries. All the security consultants are under oath not to represent any solution provider or system integrator, thus their consultancy and recommendations are most impartial.

On-site Security Survey and Audits: Conducting on-site security surveys and audits is the forte of ICISS. Its specialists have carried out numerous such surveys which were beneficial to clients in improving the security preparedness and also in cost-cutting. .

Contents Delivery: The experts of ICISS help the Clint in developing its plans, prepare manual and prepare various forms and formats to be used for every day security &safety functions. It will also help the Clients to develop the training contents such as write-ups and the presentations. The specific needs of specific niche segment of the industry will also be met by ICISS.