International Council For Industrial Security & Safety Management

Newsletter: October 2016

Let's professionalize the professionals...

Demonstrating the Value Security Brings to the Business

A Short Survey on the "Value Security Brings to the Business" was conducted recently by 'Security Executive Council'. This short self-assessment asked few simple questions about security programs. In return for the answers contacted professionals were provided with some helpful insights that successful leaders of security utilize to make the most of their metrics programs. https://www.securityexecutivecouncil.com/survey/index

Many of the items covered in this self-assessment are advanced topics in metrics that most security teams do not capture. By working through the self-assessment one can gain valuable ideas on the types of things security teams could be doing regarding communicating how much security professionals are returning to your organization.

The top scorers in this evaluation lead their security organizations by showing senior management how Security adds value to the business. The following highlights what separates the top leaders from the rest of the pack - because they have:

A security metrics program that measures value
When first initiating a security metrics program many rely on showing activity, e.g., how many badges issued or how many investigations have been completed; or a step-up, they show optimizing processes. This is a good start but the metrics that resonates with senior management are those that show a desired impact on business goals, some examples:

- Customers captured or retained, award fee contribution or client satisfaction acknowledged as attributable to proactive or reactive security measures.
- Reductions in employee interaction with time-consuming security measures.
- Reduction in cost of compliance with security-related regulations or cost to insure.
- Percent of reduction of security-related incidents attributable to improved security measures.
- Advertised and demonstrably effective security measures that enable customer satisfaction and are a potential draw for new customers and sales. Being "the secure choice" is a plus to the bottom line.
- Security department customer satisfaction survey that asks how well respondents understand security's awareness messaging and how effective the communication medium is.

A framework for scoring risk, mitigation plans and calculating residual risk
This provides a metric used by Security that measures the primary reason for having security in the organization.

A quantitative grasp on resources and capacity and articulate this to senior management
Security Leaders systematically collect, identify, analyse, and report security services and measure their business value. This process can include creating a master list of security services by program; FTE commitment by service by internal customer; criticality and/or satisfaction ranking of services by

customer; cost of security calculation by service by customer; and results reporting. The SEC calls this process a critical part of "running security as a business."

A "brand" for security and tell the brand story to a diverse set of audiences throughout the enterprise

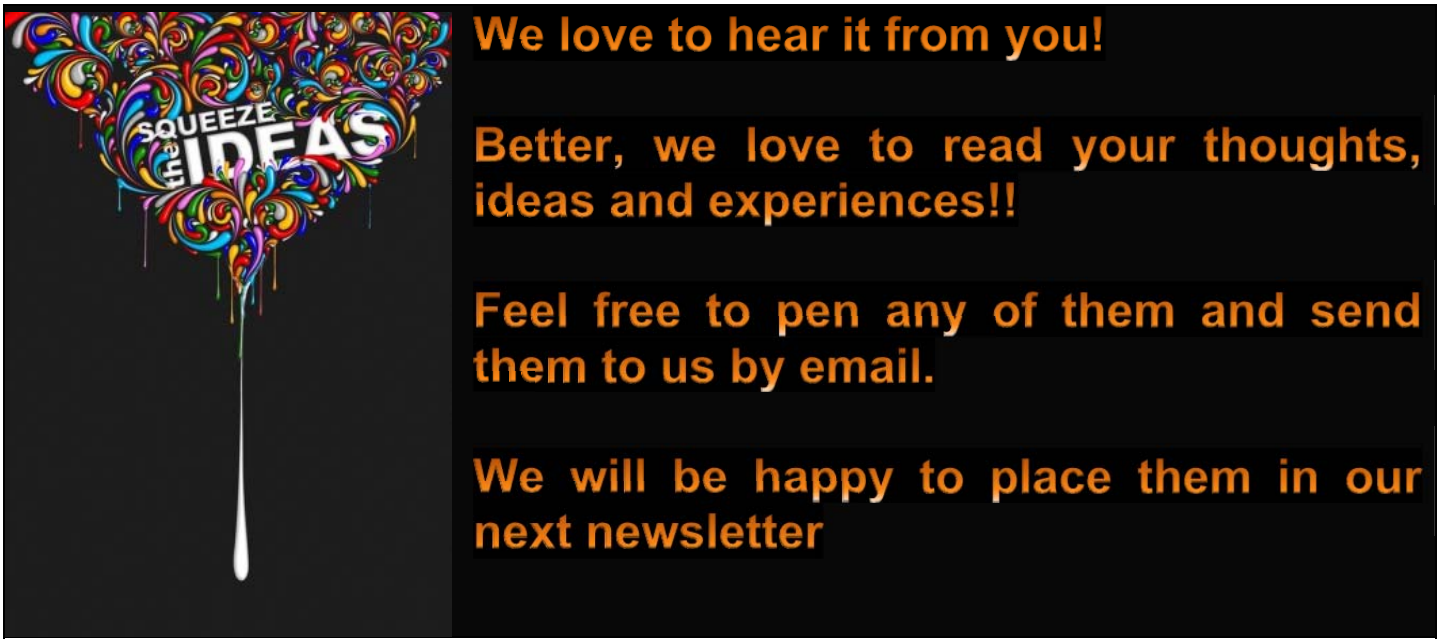
This is more than the traditional mission, vision and strategy statements. In order to brand Security as a value service, security leaders:

- Make sure security programs and services are linked to significant corporate risks and the mitigation strategy demonstrates risk reduction value.
- Show specific examples where and how security programs are aligned with the business.
- Promote cross-function team roles that need to happen for the good of the enterprise.
- Define a way that risk owners and the mitigation team can work together by identifying roles and ownership.
- Build management confidence in capabilities and long term plan of the security function.
- Have a brand value story that defines Security's philosophy and strategy in a way that builds executive confidence and support.
- Broadcast a brand value message in as many platforms as possible in the organization.
- Know the security leader is not the sole "story teller"; all of the security team can and should articulate the message

An alignment with their security services and Board-Level Risks™ and the organization's enterprise-level risk assessment

Security leaders do this to create awareness of the Board-level risks and the role and boundaries of all staff groups (including Security) in mitigating risk. Security program services are defined and mapped against the corporation's most significant enterprise risks using the language of the Board (or senior management). This often results in eliminating duplication and confusion of services across staff departments, identifying gaps in risk mitigation and fosters effective working relationships between staff groups.

They also use this alignment during Board-level presentations to show a direct connection between risks that the Board members concerned about and Security's strategy in reducing those risks – that is, the value of Security.



Malaysia's Security & Risk Environment

Maj. Prince Lazar

Prince Lazar is an experienced Security Professional, Business Analyst and Resiliency specialist with over 25 yrs. of varied experience in the Military and the Security Industry. He is well experienced in Corporate Investigations and Incident management. Prince is currently based in Kuala Lumpur and residing in Malaysia since 2007.

Prince comes with tremendous experience in the field of Threat Assessment/ Security Risk Management, Security Audit, Corporate Security, Business Continuity, Security Plan, Protective Design using the CPTED concept and knowledge on technical integration of Electronic Security systems.

Understanding the Security spectrum of Malaysia, it's worthwhile to run through a bit of the Malaysian geo-political situation & location and the typicality of the South East Asia region which Malaysia shares boundaries with a few other countries. Malaysia's location makes it less susceptible to earthquakes and tsunamis than other countries in Southeast Asia.

Within the Southeast Asia region, Malaysia is a highly open economy due to its maritime location, historically porous borders, geographic proximity to major trade and traffic routes, smaller population combined with relative affluence, shared ethnic heritages with the neighbouring countries inside and outside Southeast Asia, government policy to encourage ties with the Islamic world, and globally oriented economic outlook.

Malaysia offers lower costs in labour and land migrant workers are attracted to Malaysia because of the country's relative affluence compared with its Southeast Asian neighbours (excluding Singapore and Brunei) and other countries in Asia. Foreign migrant workers are introduced both legally and illegally. Malaysia's geographic location has exposed the country to long-distance commerce and migration has led to many transnational issues Malaysia faces today like drug smuggling and illegal workers. The porous nature of both borders and the corruption at official crossing points are both identified as causes of Malaysia's ineffective immigration management. Human trafficking is subsumed under the illegal workers category, leading the government to focus on visa violations of the trafficked victims, Terrorism and Maritime piracy.

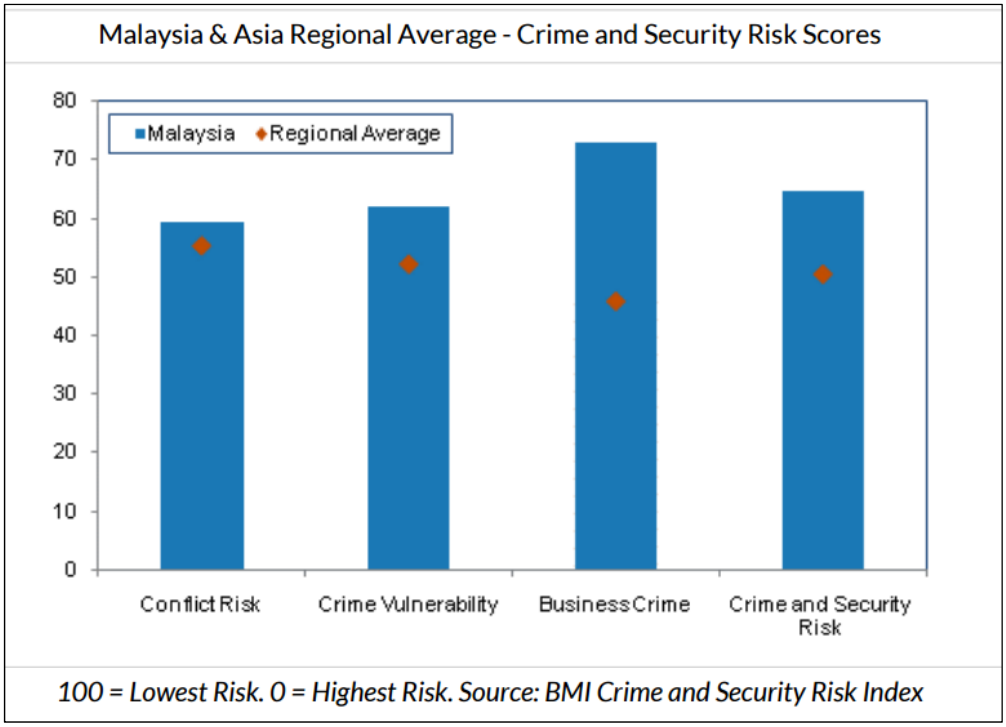
In sustaining the growth trajectory, Malaysia has become increasingly dependent on Data & Information systems across verticals like healthcare, critical infrastructure, defence, finance and technology, which are all potential targets for financially motivated cyber criminals and politically motivated actors like nation-states.

The proliferation of Wi-Fi connected tablets for sales service personnel and in-store customer Wi-Fi access are adding to the complexity of the security challenges for major retailers in Malaysia today. The retail industry is fast becoming a major target for cyber criminals. Hence, for retailers with stores throughout Malaysia, secure network connectivity linking all sites to the head office is critical to business operating processes.

Malaysia is considered to be having Moderate Crime levels although the country has seen a spurt in the Crime rates in the last few years including several reported assaults and robberies, sometimes

involving weapons but overall the Security Situation in Malaysia is considered still moderate. Other types of non-violent criminal activity include credit card fraud and automobile theft. In the list of Security concerns Crime, Kidnapping, Piracy, Terrorism, Human trafficking, financial fraud and Money laundering are among the country's priorities. Financial and organised crime is present in Malaysia, but has a limited direct impact on foreign businesses. The threat of cybercrime is growing, however, and companies must ensure they have sufficient cyber protection.

The security challenges faced by Malaysia predominantly emanates from territorial complexity and intricacies. To counter this the country has formed a Defence pact with the Five Power Defence Arrangements (FPDA) established in 1971, committing Australia, Malaysia, New Zealand, Singapore and the United Kingdom to consult on a response to any armed attack or threat against Malaysia or Singapore. The FPDA has also recently expanded its focus to address non-conventional security threats facing the region, including terrorism and maritime security.



The Territory and Territorial Seas of the Philippines, Indonesia, and Malaysia constitute a single Geopolitical space. Long-standing ties facilitate commerce and social relations among the populations of the region, but they are also conducive to transnational dissident, terrorist, and criminal activity. Vast areas lie outside government control, and ethno-national, ideological, and religious conflicts exacerbate the void in governance. The threat from kidnapping has become a serious issue in Maritime Piracy which is predominantly prevalent in East Malaysia, particularly in the islands off eastern Sabah due to its proximity to the Sulu archipelago in the southern Philippines. The tri-border area (TBA) between the Philippines, Malaysia, and Indonesia is a key hub of terrorist and related criminal activity in Southeast Asia, a well-known transit zone for weapons and explosives, and a principal logistical corridor for local and transnational terrorist groups.

Terrorism has increasingly become a big threat in Malaysia off late and it remains a potent Risk due to the Islamic influenced groups operating in the Region and Middle-east. While previous terrorist organisations were disparate organisations fighting for separate causes, the regional terrorists may get-together to fight for a common cause across national boundaries and will possess capabilities to target masses using easily-acquired advanced technology weapons or equipment. The insurgency in the Southern Thailand by the Muslim Thai rebels who are active along the Thai border has also further increased the threat of Terrorist attacks in this region.

International terrorists are suspected of operating out of Malaysia from some time and the growth of Muslim extremism has spurred the development of home-grown terrorist groups and dozens of disparate fundamentalist groups / cells are believed to be operating in the country. The terror threat to Malaysia, however, doesn't stem from a particular IS Terror outfit but by the presence of regional terror groups like Abu Sayyaf, the Moro National Liberation Front and many insurgent (terrorist)

organizations which have always posed a threat to Malaysia's northern state of Sabah, and now with their given allegiance to IS, the threat has become more potent.

Malaysia has taken a strong stance on terrorism with the increased terrorism threat; however the counterterrorism posture is still driven by domestic political considerations. Malaysian authorities have arrested several individuals for activities linked to IS. They have also been very proactive, especially in terms of monitoring flight manifests, preventing people from traveling to and from Syria and Iraq and monitoring social media.

While Malaysia's counter-terrorism capabilities are relatively strong, the risk of political violence remains high due to tensions between ethnic groups. Over the last five years, Malaysia has experienced an increased number of demonstrations over political divisions, racial/religious tensions, and international developments. The country's recently implemented Security legislation introducing indefinite detention without trial has the potential to foster discontent and trigger violent protest.

Another growing aspect of Security problem is the threat posed to Tourism industry in Malaysia. With the rise of Tourism industry and Malaysia being known as one among the top tourist destinations in the region, it receives a high number of tourist arrivals which has increased the issues of safety and security in tourism industry such as crime, terrorism, food safety, health issues and natural disasters as the main concern.

Malaysia - Crime and Security Risk

	Conflict Risk	*Vulnerability To Crime*	*Business Crime*	*Crime and Security Risk*
Malaysia Score	59.3	62.0	73.0	64.8
Asia Average	53.4	52.3	46.0	50.6
Asia Position (out of 35)	15	12	5	8
Global Average	49.2	50.1	50.0	49.8
Global Position (out of 201)	70	73	41	54

100 = Lowest risk; 0 = highest risk. Source: BMI Crime and Security Risk Index

The security industry in Malaysia especially the Guarding sector with around 24,000 registered Private security guards is saddled with problems with issues of employing incompetent, unqualified and unfit guards. There is a need for a comprehensive review of the security industry in the form of a proper Security framework & regulations. If Private Security companies (PSC) can be regulated and they co-ordinate well with the government institutions they can be a source of tremendous information and can help the police track down criminals and assist in larger law and order maintenance.

Public and private sector organizations are investing in several areas to ensure that their economic rise does not slow because of infrastructure disruptions brought upon by cyber sabotage or terrorism or lost revenue because of intellectual property theft. There is an increasing emphasis on security Awareness, training & certifications and Academic institutions are also focussing on specialized training and certification courses specific to Security & Safety. Security based job programs such as internships are in place between the academic institutions, government organizations and the private sector which is a positive boost to Security. This manifests in strong information sharing between public and private sector organizations and a general openness amongst organizations, even competitive organizations, when it comes to combating cyber-attacks.
Going with the economic growth in the last few years in Malaysia, from securing the physical borders & assets to endpoint and data security, there is a good trend in a holistic approach to security. Security in Malaysia has seeking an approach from the perspective of: What can be done, What

technology / solutions are available, and How it can be employed for end-to-end controls which is a healthy sign towards Security. When vetting solutions, security consistently makes it into the top three on the list of must-have requirements.

The total Malaysian safety and security sector is estimated at US$2 billion and is expected to grow. Private consumption of safety and security equipment has also risen over the last decade mainly due to the increased rate of urbanization, a growing middle class owning assets which they wish to protect and a lack of faith in the local law enforcement (*Source: Global Safety & Security guide US COMMERCIAL SERVICE*). The Revenue in the "Security" segment in Malaysia amounts to USD 1.1 million in 2016 and the revenue is expected to show an annual growth rate (CAGR 2016-2020) of 46.94% resulting in a market volume of USD 5.3 million in 2020 (*Source: Statista market research portal*).

Public consumption is mostly government initiated purchases for the maintenance of law and public order, which is long and tedious process. On the private consumption it is usually driven by purchases of new homes, cars and other assets that the common consumer wishes to protect. Until recently, most consumers based their selection process purely on price. In the last five years, there is a significant change in attitude and mind-set of consumers whereby quality and reliability also play a major role in selecting the type and brand of security products to invest in. The demand for technologies to keep users updated on the status of their security system. These usually include remote access via smart phones through internet, instant notifications via SMS and/or monitoring companies. New solutions like intelligent video surveillance and cloud security devices are also gaining popularity, especially among the more affluent segments of the market.

US companies presently dominate the Malaysian market for both the public and private market segments. However, Chinese and German companies are fast gaining footholds in the market, especially for point of entry equipment and for the private consumer market, Taiwanese and Chinese are eroding US market share with newer and price competitive surveillance and prevention systems.

Malaysia with diverse ethnicity, race & language faces dynamic Security issues and challenges. This calls for maintaining a secure environment in the country, providing opportunities for economic development and better stability.

Cell Phones Become Fraud-Fighting Tools

Mobile phones are finding increasing use as weapons in the fight against credit card fraud thanks to new services. Technology developed by Ericsson allows people to be located and credit card transactions assessed as fraudulent by using mobile network information to pinpoint a cell phone on most networks worldwide. The technology enables card firms to verify in seconds whether a customer is in the same country where a specific transaction is being executed, and it is particularly useful in instances of overseas credit card fraud in high-risk countries. Meanwhile, MasterCard and mBlox have partnered to deliver a service in which text messages are immediately sent to bank customers to confirm high-risk credit card transactions.

MasterCard calculates that its service will let banks send as many as 10 messages for every phone call placed to verify credit card transactions. This response speed means that cards can be blocked in a matter of minutes, lowering the volume of fraudulent transactions. Meanwhile, Visa Europe is conducting a pilot of a new mobile service that transmits consumers' instant transaction confirmation to their cell phones when they use their debit, credit, or prepaid cards. Cardholders can opt to receive a text or email alert on any mobile device or to an application downloaded to a smart phone. When a credit card transaction transpires, the service instantly sends the time, location, and amount of each transaction to the cardholder's handset.

The Virtual Reality between Call of Duty & IS Activities

Yuvraj Bhushan

Note: The author of this piece - Yuvraj Bhushan is Class 11th Student in Delhi Public School, Greater Noida. Priding himself to be a 'gamer', he often draws interesting comparisons between visual realities and ground realities. He once boastfully declared that he can easily prepare strategy to annihilate Islamic State! When challenged to prove his point, he shared that the story line of the famous game – 'Call of Duty' is the one which IS is following to its last Y! When he explained from episode to episode the similarities in the game and horrifying activities of IS, I was knocked out! There has been no tampering with the language Yuvraj Bhushan used to retain its rawness!
Could it be true! Is Islamic State really following the story line of this game Call of Duty? Read on…

While playing the game of "Call of Duty' and also watching world news a thought struck to me that this one of the most famous games in the world "Call of Duty by Infinity Wards" is being used as storyline to what the infamous terrorist group Islamic State is doing to the world right now.

Those who have experienced and played Call of Duty (Modern Warfare Series in particular) are familiar with the game's storyline and know about the similarities which are found in IS's planned attacks which are carried out till now.

To understand this more briefly, let's look into facts.

The Storyline.....

As we look into the storyline of the game we will notice that it is similar to the US invasion on Iraq during Saddam Regime. US forces fought in Iraq which led to huge military and non-military Casualties and deaths. After the war In Iraq, US leaves the country devastated with political and social unrest between Shia and Sunni Muslims which lead to the formation of a terrorist group known as ISIL (now known as ISIS).

As we follow the facts and the storyline, the Russian forces intervened and everyone knows that Russia and USA have always been in conflicts due to different reasons Since World War 2.

With War driving the country to destruction, the war (in the COD storyline) shifts to US and Russia. With the two forces engaged in warfare, the Terrorist group (in game) takes advantage and Target countries like Afghanistan and Syria and become successful in dominating them. This in fact is true

as ISIS dominates Syria, Iraq, Iran and some parts of Afghanistan Due to similar reasons to the game. The conflicts in real world between Russia and America are just one spark away!

As the story continues, the terrorist group in the game targets European countries like England, Paris, India, Russia. The terrorist in the game are also successful in Assassinating political heads like the prime minister of Afghanistan and Iraq to gain dominance in region.
Attacks then shift on European Countries. Paris Attack and Attack on Charlie Hebdo can be taken into account. ISIS possesses possible nuclear weapons which pose threat to many countries. The game character Makarov can be related to the ISIS leader Abu-Al-Bakr-Baghdadi, the self-styled Khalifa!

The reason for the turning of tables between US and Russia (in the Game) was an undercover agent working for the US CIA with terrorist group (In the game) which carried out the attack on the airport in mission “No Russian”.
In the game, the undercover agent - PFC Josef Allen is murdered by the terrorists he was working with and is left at airport after the success of the attack. The Russians after finding the body of the American at the Airport believe that attack was planned by America and hold US responsible. The main motive of the attack was to turn US and Russian against each other.

Attack on Brussels Airport

The Attack on the airport in Brussels was very strategically planned for maximum causalities. ISIS was blamed. If anyone played the game, they will find the mission “no Russian” to be similar to the attack.
It is Possible that the groups like ISIS may be using video games like ‘Call Of Duty’ to mentally train their fellow terrorists to carry these attacks or may be using them in planning these attacks. Recently, ISIS has uploaded a new video showing the fall of Eifel tower. The video was taken from Call of Duty Modern Warfare-III

Call of Duty (MW-3) is the latest part in the modern warfare series and probably the best part. In this part the destruction is on its peak with war waging in every major country, the stock market crashes and riots create problems for law enforcements.

Russians attack its rival US with full military force by deploying its troops on US soil. This proves as yet another advantage to the terrorist as they get an opportunity to further strengthen their hold in central Asia and also infiltrate many other European countries. However, at the end of war, deaths are countless and much of the world is devastated with the ruins of war.

PREPARE FOR THE FINAL ASSAULT

Real Facts

- **The environment in the game is similar to the environment developing in the world with war tearing countries like Syria apart.**
- **The attacks on Brussels airport and Paris may have been planned using video games.**
- **It is Possible that the groups like ISIS may be using video games like 'Call of Duty' to mentally train their fellow terrorists to carry these attacks or may be using them in planning these attacks.**
- **Games like 'Call of Duty' are being used by terrorists to train their recruit jihadis and develop streak of violence in other fellow terrorists.**
- **The story of the game may soon become a reality as it is a fact that ISIS is advancing towards Europe and has already sent THEIR undercover agents hidden among refugees entering these countries with fake passports.**
- **It is Possible that the groups like ISIS may be using video games like 'Call of Duty' to mentally train their fellow terrorists to carry these attacks or may be using them in planning these attacks.**
- **They are already acting like Recruiters, planners, suppliers etc.**

Establishing a Safe haven

Follow three basic steps in setting up a safe-haven in your home:

- Designate an internal room;
- Install a two-way communications system or telephone; and
- Furnish the safe haven with an emergency kit.

It is highly unlikely you would spend more than a few hours in a safe haven; however, the supplies listed below are suggested for your maximum safety. Your security officer can tell you more about how to select and secure your safe haven.

The following is a checklist of possible safe haven supplies.

- Fire extinguisher
- Fresh water
- 5-day supply of food
- Candles, matches, flashlight
- Extra batteries
- Bedding
- Toilet facilities
- Stove, fuel
- Shortwave or other radio
- Medical/first aid kit
- Other items for your comfort and leisure--a change of clothing, books, games.

Forthcoming Event

SECURING INDIA 2016

Roadway to a Secured India:
Smart Borders, Smart Policing and Smart Security

8th Edition of SWI's Annual Conference & Exhibition on Internal Security in India

3-4 October2016, Hotel Le Meridien, New Delhi

Organised by: SWI security watch india

SWI Invites you & your Colleague to the Largest Gathering of Security Technologies and Experts

THOUGHT LEADERS:
Learn from Experts & Advisors (Partial List)

Mr. Harry Dhaul
Director General
SWI

Gen J.J Singh
Former Governor of Arunachal Pradesh, Former Chief of Army Staff and Chairman Advisory Board, SWI

Lt General Syed Ata Hasnain (Retd.)
PVSM, UYSM, AVSM, SM, VSM & BAR, Faculty, The Institute of Peace and Conflict Studies (IPCS)

Maj. Gen. G. D. Bakshi (Retd.)
Editor
Indian Military Review

Shri. Gopal Pillai IAS (Retd.)
Former Union Home and Commerce Secretary
Government of India

Col. Sandeep Sudan
Head – Special Services Group, Reliance Industries Limited

Mr. Raghu Raman
President, Risk, Security and New Ventures
Reliance Industries

Mr. Shyam Ratan Mehra IPS (Retd.)
Former Secretary Security
Government of India

Mr. Arup Patnaik, IPS (Retd)
Former DGP Maharashtra and Former Commissioner of Mumbai

Mr. Maroof Raza
Mentor
SWI

Mr. Shiv Charan Yadav
President, Asian Professional Security Association (APSA)

Supported by

ICISS
International Council For Industrial Security And Safety Management

15% Special Discount for ICISSM Members on Delegate, Exhibition & Sponsorship Fees

---

ICISS at LinkedIn: http://www.linkedin.com/groups?gid=4413505&trk=hb_side_g
ICISS at Google Group: https://groups.google.com/forum/?fromgroups#!forum/icissm

Suggestions & feedback to: onlineicissm@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!