SEPTEMBER 2022

VOLUME 08

The IISSM News

The International Institute of Security and Safety Management

Editorial

Dear Readers,

Greetings to you all!

This year too, rains did not start receding from 17 September, which is an established date in the calendar of Indian Meteorology Department (IMD) wherein the South Western Monsoon starts fading away from the Indian peninsula. On the contrary, heavy rains were lashing half of the country especially Northern Half and it is being said that this is not yet over, at least mid of October, a clear shift of a month. It also reminds us that this year arrival of summer started in March itself. While talking about rains, Bengaluru was being ridiculed about couple of weeks back in Social Media platforms because of deluge and certainly people had a tough time. It was even being touted that e-commerce company techies ensure that a product can be delivered at your doorstep within half an hour (anywhere in the globe) but they themselves need five hours to reach office. By the time social media posts cooled down, again it was flustered with the images of drowned city of New York, USA and last week only it was replaced by Delhi NCR.

So much on rains and impact of climate change. Well, we can write, talk and raise voices across the global platforms and shout at the politicians, administrators, land mafia, real estate developers and least the municipal committees on their actions or inactions. We can debate till cows come home on this issue. But we need to ask one question to ourselves as well and that is have we done our bit? Have we reduced usage of cars even for small household shopping, reduced the usage of air conditioners or let's say have started going for groceries and provisions walking or by cycling! Then how can we blame others and finally the Mother Nature, whom we have misused over and over.

Coming back to 17th Sep, this year too it has again made its mark on the pages of history of Wildlife Preservation, coinciding with the birthday of our Prime Minister Narendra Modi. We got the first tranche of Cheetahs from Namibia and were released in Kuno National Park in Madhya Pradesh (India) by the Prime Minister himself. This may appear to some people that it is politically motivated blah.. blah, but certainly a Red Letter Day in the history of wildlife preservation. In the past, India has succeeded in preserving the fast vanishing numbers of Tigers and Asiatic Lions within few decades. For Cheetahs, it took 75 years since its extinction from Indian landmass (in 1947), to return into our Jungles and we sincerely hope that India will have sizable numbers all across the country.

Last year on this day only, we made a world record in vaccination efforts (for Covid-19) by vaccinating 1 Cr. People. This event has almost been forgotten because we have left the trauma behind and moved on. Due to this cruising speed, we have achieved the herd immunity. But we have one major concern and that is Lumpy Virus among the cows. This has impacted Rajasthan state and it is no denying fact that a big threat is lurking around, hope it doesn't get transmitted to human beings.

This is also the beginning of the festivity season in India, starting from last week September with Navratra (this year) and celebrations will continue till the end of Holi.

At the end, we wish you a very happy Deepawali.

Jai Hind!
Col (Dr.) MP Sen

CONTENT

CELEBRATING
THOUGHTFUL
SECURITY!

Godrej

FUTURE READY SOLUTIONS, TO SECURE YOUR PRESENT.

Burglary and Fire Resistant Safes | Vault Equipments | Strong Room Doors
Currency Handling Equipments | Access & Entrance Control Solutions | Marine Equipments

Quality Assurance
Highest quality products and services

Design and Technology
Indigenously designed & technologically advanced products for security, safety & protection

Comprehensive Range of products
A complete gamut of security products & solutions

Global Presence
Broad geographical footprint

Renowned Indian & International Certifications

121 YEARS LEGACY | Bureau of Indian Standards | Sweden | Germany | USA | France | Germany | UK

Godrej & Boyce Manufacturing Company Limited, Plant-17, Pirojshanagar, Vikhroli, Mumbai - 400079, INDIA.

Toll Free: 1800 209 9955 I Email: secure@godrej.com I Visit: www.godrejsecure.com

Announcement: 32nd IISSM Annual Global Conclave

The IISSM's Annual Global Conclave, the 32nd, will be organised on 18-19 Nov 2022. This year too, the Conclave will be held on virtual platform. The overarching theme for the conclave is **"Security, Safety and Loss Prevention : An Enabler to the Nation Building".** There will be four Keynote addresses and four Panel discussions each, details of the Conclave topics are given in the Invitation flier (added in this edition).

Certified Security Practitioners' Course (VC) (20-21 & 27-28 August 2022)

The Certified Security Practitioner Course has been conducted by IISSM (20-21 & 27-28 August 2022 Weekend Course) on virtual platform. The participants were from Delhi NCR, Ahmedabad, Vishakha Pattanam and Bangalore. The sessions covered the topics like Concepts Corporate security, Fire safety Management, Risk Management, Disaster Risk Management, Fire Safety Management and Evacuation (National Building Code and NFPA Standards), IEDs and Bomb threat handling, Technological Application in Security Management, Bank, Hotel, Mall and Hospital Security, Incidence Response System & Crisis Management Framework, Corporate Vigilance - Overview & Preventive Aspects, Arms Act and Arms Licensing, PSAR Act - 2005 - Need for review, Executive Protection and Role of PSOs, Cyber Security & Data Protection, and Business Continuity Planning. In addition, a Class Room Crisis Simulation Exercise, on Flood Situation Management was conducted which was highly appreciated.

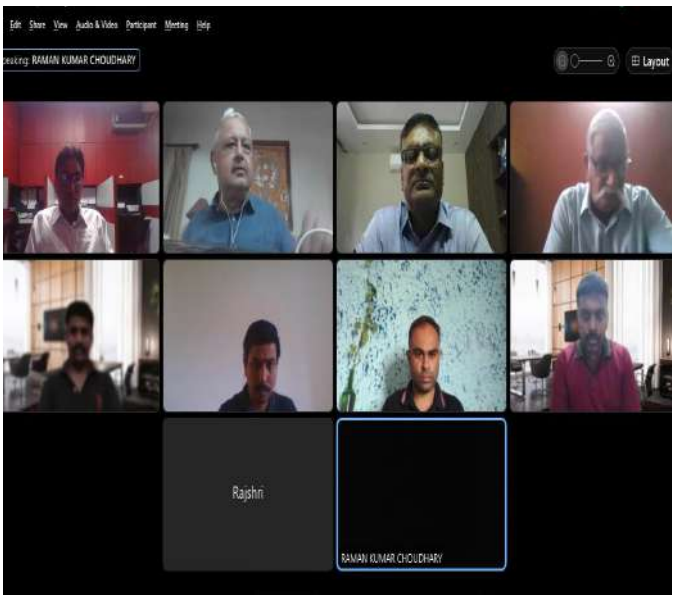
The Faculty Members who conducted the Course were:

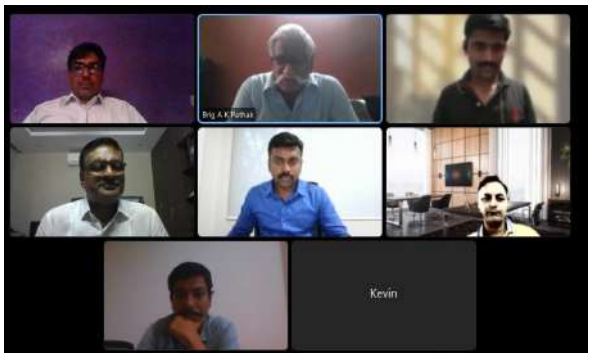
Brig A K Pathak (Retd) &
Col (Dr.) M P Sen (Retd): IISSM Faculties
Brig (Dr.) VK Dutta (Retd) &
Col Sumit Monga (Retd) : Guest Faculties

Quotes from Participants on Overall Assessment of the Course are mentioned below:-

Mr Prabhakaran G, Key Accounts Manager, Commscope, Bangalore
"I was looking for a training program since long specially the way IISSM conducts the sessions….methodology of teaching and quality of training were superb"

Mr Kevin Domadiya, Security & Loss Prevention, Amazon, Ahmedabad
"It was very nice program, where I learnt so many new things and enhanced my knowledge".





CYBER CHALLENGES FOR MOBILE USERS & RISK MITIGATION

Wg Cdr Raman K Choudhary
CSP Aug'22 Batch

INTRODUCTION

Development of mobile technology has enabled mobile devices to be adopted in daily activities. Especially Financial institutions are adopting mobile devices for banking purposes to enable their clients to bank from anywhere at any time. Although, the adoption of mobile technology enabled convenience to the users, it has brought about a great security challenge. This paper reviews the cyber security challenges to mobile users and ways which minimize the impact. Findings indicate that some mitigation strategies to cyber threats

to mobile users are in place though they seem not to address the major challenges. Historically, the first mobile malware was reported to have been generated in 2004, but it is only in last three/four years that it has become a serious threat to the end users. The rapid growth in smart phones and tablets over the years has led to the inevitable rise in targeting of these devices by cyber criminals.

GROWTH IN SMARTPHONES & TABLETS

With mobile subscription worldwide totaling approximately seven billion, it is clear that mobile devices are rapidly replacing Personal Computers (PC) at home and in the work place. We now rely on smartphones and tablets for everything and internet has almost started regulating our lives i.e., from web surfing to e-commerce transactions and online banking, ticket booking to e gaming. Therefore, in the recent years, mobile based malware has transformed from an emerging threat vector to a serious one and being consistently exploited by cyber criminals.

ANDROID VS IOS

Mobile malware writers know that the best way to infect as many devices as possible is to attack central applications market. Therefore, today the most likely way that malware will find its way on to a mobile device is through downloading a malicious application that hasn't been sufficiently vetted. Cyber criminals plant applications that may include hidden (obfuscated) malicious functionalities in an attempt to avoid detection. Inevitably Google's Android platform has become a much greater target for mobile writers than Apple iOS because unlike Apple, it doesn't employ a 'walled garden policy' with regard to application.

APPLE

Apple's Walled Garden Application Store, where applications are fully vetted before being made available to customers has prevented widespread malware infection of iOS users. As a centralized point of distribution, the Apple store provides users with confidentiality that the application they download has been tested and validated by Apple. Evidence of malicious malware showing up in the Apple store is negligible. However, it's safe to assume that since Apple does not make APIs (Application program interface) available to the developers, the iOS operate system has less vulnerability.

GOOGLE AND ANDROID

Like Apple, Google provides a centralized market for mobile application called Google Play. However, that is offset by the Android's ability to install application from third party sources such as Amazon. Others originate from malware hotspot like Russia & China. The criminals develop, deconstruct and decompile popular application like Angry Birds and publish malicious versions make them available for free. Similar is the case of MS Windows. Last years a new form of banking malware was detected that combines conventional browser attacks against windows with social engineering designed to compromise Android devices and complete the theft via smartphone. To intercept

user information.

THE CORE MODUS- OPRANDI

The basic modus operandi includes the injection of malware code into internet explorer and there after capturing browser personal information and cookies. The injected code even blocks users from accessing their accounts un-till the smart phone malware has been installed and provided an activation code. Once the activation takes place all the transaction details are available with fraudsters to mount the attack.

CYBER SECURITY CHALLENGES

Several organizations encounter the challenges brought about by cyber-attacks. Cybercriminals have sought to infiltrate organizations' databases by hacking into their networks. It is further stated that a survey by audit firm Price water house Coopers found 33 per cent of firms had been affected by cybercrime in the last 24 months, and a third of them suffered significant financial impact. In addition, the Ministry of Information, Communication and Technology reported an increase in cyber-attacks by 100 per cent in 2014 over the year 2013. The cyber security challenges identified are as follows:

Inadequate Technical Skills.
The insufficient technical skills, both at management and board levels are a challenge to secure mobile service provision in today's changing world. According to Computer Emergency Response Teams (CERTs) are valuable assets for performing the cyber security functions, but they are either lacking or in nascent stages across World. It is further stated that without the capable Computer Emergency Response Teams in place with the appropriate technical expertise the networks are more vulnerable to cyber threats, making the users vulnerable to attack and fraud.

Lack of Awareness.
Awareness is very important in realization of total cyber security. The mobile phones adoptions and applications like mobile money have enabled users with little prior experience with technology to own them. Users having limited digital literacy have a more likelihood to be unaware of cyber threats, which places themselves and the networks at greater risk. The lack of cyber awareness is a leading cause of infection across the globe.

Legislation.
The legislation specifies the roles to be undertaken by the government which include: creation of the policy and legal framework for development of cooperatives, improvement of the growth and development of cooperatives by providing requisite services for the organization, the registration, the operation, the advancement and dissolution; and the development of partnerships with cooperatives through consultative processes which are focused on legislation policy and regulation. Because the cyber environment knows political boundaries, international cooperation on cyber security issues is necessary, but few African

countries engage in cross border law enforcement efforts.

Low Prioritization.
The cyber security state is hindered by the low prioritization from national leaders. This is mostly attributed to the limited resources which must first be allocated to address the society's problems which are most fundamental. Thus, the low priority for cyber security in the face of some other pressing issues endangers vulnerable networks and their applications. This makes the organization least safe place for operating a sensitive application like mobile money.

Poor Technical Design.
Technically expert adversary can take advantage of poor security design within mobile money apps or simply by pass poorly implemented encryption. For example, a mobile application could track all the purchases made by the target illegally, then gives the adversary information about the target's strategies. Also, a mobile application can make random purchases on behalf of the targe. When performed in an inconspicuous fashion, such purchases would unlikely raise alarms in fraud detection systems.

Social Engineering Practices.
Social Engineering is considered as the greatest security threat for people and organizations. Cyber-attacks on organizations have been rampant over the past years. Organizations are however getting smarter and putting in place systems to curb cyber-attacks, making it more difficult for hackers to gain access. Thus, the only fraudster's soft spot left is the human mind. To gain access to an organization's sensitive information, such as client passwords or account details, the criminals have resorted to social engineering. Some of the techniques used include Phishing, Reverse social engineering, shoulder Social Engineering is a process of deceiving people into giving away access or confidential information. According to define social engineering as a diverse and complex technique for gaining unauthorized access to confidential proprietary and personal information. According to Social Engineering is a method of gathering information and performing attacks against Information and Information Systems. Social engineering attacks are multifaceted and include physical, social and technical aspects, which are used indifferent stages of the actual attack. Social engineering tactics are used by criminals because it is easier to exploit a person's natural inclination to trust. According to Social Engineering is phishing, surfing, baiting and eaves dropping discussed as follows:

Phishing.
Phishing is the process of enticing people into visiting fraudulent web sites and persuading them to enter their personal information on the same. An e-mail or text message is sent by a phisher that appears to be coming from a legitimate bank, school, company or institution. According to, in

phishing, the consumer receives an e-mail indicating that there is a problem with the account. The authors further argue that instead of the e-mail to provide a fraudulent link to click on, it provides a customer service number that the client must call and is then prompted to log in using account numbers and passwords. Phishing attacks can also be conducted via email, phone calls, text messages and fax, as well as other methods of communication, including social media. Phishing is defined by: to be an exploit that is generally defined as impersonating a trusted third party by a phisher in order to gain access to private information. In such case, the phisher sends an email that appears to come from a legitimate business or individual requesting verification of information and warning of terrible consequence if it is not provided. Usually, the email contains a link to a fraudulent web page that appears legitimate, sometimes with company logos and content and requests private information. Further it states an example which is spear phishing, in which the attacker initially gathers personal information about the target victim and uses it to tailor the phishing scheme, which increases the probability of success.

Reverse Social Engineering.

Reverse social engineering is a sophisticated form in which the attacker creates a situation in which the unwitting victim believes that the attacker can help solve a problem. Social engineering consists of three major parts: sabotage, advertising and assisting. The first step is sabotaging the company's computer system which can range anywhere from disconnecting someone from the company's network to sophisticated manipulation of the victim's software applications. The attacker then poses as a technical aide to fix a problem that the attacker created or that does not exist. The attacker communicates his capability to help, such as through advertising or a phone call. Finally, the victim invites the attacker to assist, which eventually allows the attacker to access to the desired information.

Shoulder Surfing.

Secret information should be protected from sensitive and various applications by use of secured authentication system. This is because the vulnerabilities of textual passwords such as short passwords are easy to remember, which makes them vulnerable for attackers to break. Shoulder surfing is stealthily looking over the shoulder of someone who enters security codes or passwords.

Baiting.

This is an exploit that uses malware infected physical media such as CD-ROM, USB drives etc. to achieve an attack. Looking legitimate, the Trojan horse relies on the curiosity or

greed of the victim who finds and uses the device, enabling installation of the malware on the targeted organization's internal computer network. In order to increase the chances of success of such attacks, the perpetrators often try to develop a relationship with their future victims. According to survey in last decade, the most prevalent type of social attacks is performed by phone.

Eavesdropping.
Eavesdropping is unauthorized information capturing for example usernames and passwords leading to compromise in the confidentiality. Communication in a mobile device is over a wireless network. The confidentiality and integrity of the communication can be compromised by the means of eavesdropping, man in the middle attack or by spoofing because the communication goes over the air. When information is manipulated, it compromises the integrity of the data.

RISK MITIGATION TECHNIQUES

Approaches to Securing Mobile Banking Service Provision In order to effectively defend against cyber-attacks, a multifaceted approach needs to be used. This can be achieved through physical security mechanisms, technical controls, security policy and education and training. A few of the physical/ technical techniques/controls are:

Access Control.
Physical security must be properly implemented because many attacks succeed through gaining physical access. Therefore, access control must be put in place to allow authenticated users to gain access and keep the rest off.

Double Passwords.
According to, double passwords control can help a great deal in the war against physical insecurity. The double password control includes the log-in password and the transaction password. For the log-in password a mixture of numbers and letters needs to be used and this means confidentiality is ensured to a certain degree and this is limited to log in. The transaction password on the other hand is required when users need to transfer funds.

Technical Controls.
Proper technical controls can help reduce the social engineering risks. One of the technical controls that can be employed is the use of firewalls. According to, firewalls employ a combination of computer hardware and software that is designed to separate the Internet from the Internal Web servers, networks, computer systems and databases securely. Back-up and recovery is another technical control. An off-site back up is required for recovery from major failures to ensure continuity in business operations.

Security Policy.
Security policy is the key and most important element of a good defence against social

engineering because it can take out uncertainty which is what social engineering depends on. In an organization, the written security policy document provides a very high-level description of the several controls the organization uses to protect information. Also, the strength of any system is not greater than its weakest link. Thus, protecting information that is confidential in an organization is a business and legal requirement. With financial resources justifiably limited, leaders are required to take policy actions that will increase the user trust without requiring exceptional monetary and other resource allocations. This may take into consideration the information like licensing for mobile money services to include explicit rules for the collection and sharing of personal information. Review of policy at regular intervals is must.

Education and Training.

People's vulnerability to social engineering is described in terms of their awareness to the types of social engineering attacks. Therefore, people need to be educated and trained constantly to be resistant to social engineering. Improved knowledge of threats is often cited as critical to enhance cyber security. Financial institutions try to educate their customers, in part through new channels of communication such as Twitter and YouTube, in addition to more frequent website updates. The financial institutions are required to educate their security personnel and their end-users on a continuous basis. Nations are required to commission public awareness campaigns which are focused on cyber security and personal data.

CONCLUSION

Threats to mobile devices are persuasive and ever escalating to the users through malwares. Realizing user perceived secure mobile free from cyber-attacks is a dream. Several attempts have been put in place to mitigate the challenges encountered in effective provision of user perceived secure mobile usage, nonetheless, much is required to be done. However, they have not address all the challenges encountered. A major omission observed in the cyber threats' mitigation strategies is the lack of a dedicated financial plan in order to achieve all the identified strategies. With training, education/awareness drives and strict implementation of Standing Operating Procedures (SOPs): individuals and organisations can cost effectively guard against current and emerging threats, while retaining optimal efficiency and flexibility in their usage of mobile devices.

About the Author:

(Wing Commander Raman Chowdhary is a Veteran Air Warrior, has served the country for almost 25 years on various Command and Staff assignments. He has had hands on experience of handling Aviation Base Security and Administration specially in sensitive areas. He has attended CSP course in Aug 2022.)

Aviation Security and Role of Private Security Agencies
(A Success Story of the Study Lead by IISSM)

Hiranya Mohanty

Introduction:

Today, India has become the fifth largest economy and has been experiencing a surge in air travel requirements that too from non-metro cities to metros and vice versa for business, health, and other reasons. The government also came up with plans to develop airports in tier-2/class B or C cities and towns in India. While this initiative will boost the economy and business, it comes with additional challenges and opportunities. One of these is the security of these airports and the extra burden on the exchequer for providing this security. While, the Central Industrial Security Force (CISF) and other paramilitary forces as well as the state police forces are deployed in most of the metro cities and state capitals, deploying them in approx. 700 cities are not only a big challenge in terms of scalability, but in terms of cost and operational viability. As airports at metros have tremendous footfalls on a 24x7 basis the situation in smaller cities is quite different as there will be fewer fights and thus a lower turnover, resulting in higher travel and cargo costs. Given the high cost of airport security, such airports could be economically unviable thus defeating the very objective of increasing the air travel network in the country.

The cost of security through a full-fledged Paramilitary Force like the CISF is very high because of its organizational setup, weapon holding, training, and other issues associated with a regular armed forces unit. While they are a formidable entity ensuring security 24x7, many of the functions that they are deployed for can be performed by suitably trained private security personnel at a much lower cost.

All the airports in the country, existing ones and the proposed ones, cannot be covered with the existing manpower in the CISF, and therefore the need was felt to carry out a study to address the security requirements of small, medium, and large airports in the country to reduce the cost of security at these airports albeit without losing operational efficiency or compromising core security functions. Thus, the Ministry of Civil Aviation requested the International Institute of Security and Safety Management, an autonomous, not-for-profit training institute that is an ISO

9001-2015 certified centre of excellence in training in security, safety, and loss prevention (IISSM) with a standing of 32 years to conduct a study to suggest suitable measures broadly with following aims:

(a) Establishment of security grid for the upcoming airports across India.

(b) Cost of raising new CISF battalions and time frame that is required to cover approx. 700 airports within the country.

(c) Can some of the tasks be outsourced to third-party/private security agencies?

(d) Cost of manning these small airports with private security guards w/o losing operational efficiency and at an acceptable cost.

(e) Can there be an alternative to CISF deployment, where and in which form etc.?

The IISSM in turn set up a team of internationally acknowledged experts in aviation security and launched a comprehensive study of airports of all types in the country and in the USA, Canada, and Australia to ensure that the best practices adopted internationally were incorporated in its report.

The International Institute of Security and Safety Management (IISSM) was entrusted with this task because of its expertise, leadership, and reputation as a Think Tank in the domain of Private Security. The team was led by Mr. Rajan K Medhekar, IPS (Retd), former Director General of National Security Guards, and the current Director General of the IISSM.

The study was conducted extensively covering the following:-

- What is the existing setup in all types of Airports in India?
- What is the future requirement of security in all these airports?
- Threat Perception and Analysis of Resources.
- Cost of the Security in Metros and Non-Metro/Class B/C City Airports.
- Can the CISF or paramilitary forces undertake the responsibility in all the airports and the cost thereof?
- If 'NO' then what time and cost are required to raise additional forces?
- Is there a need for deployment of highly trained force in all airports/in all types of tasks?
- Can there be a possibility of outsourcing some of the tasks to third parties?
- If Yes, then in which types of tasks can be performed by them and the cost thereof.
- Would it be a failsafe arrangement? Will core security requirements be compromised or diluted in any way?

- Can the private security agencies in India undertake these tasks?

- Is there a precedence for deploying Private security Guards anywhere in the world?

- Other miscellaneous related issues.

The team travelled extensively and based on their observations they deliberated on these issues for months, studied global aviation security costs, deployment, type of forces and tasks thereof, and the role of Private Security agencies (if there are any). The study team finally submitted its report with 22 recommendations.

The study team after long and due deliberation suggested that Private Security personnel, adequately vetted and trained, can be employed in almost all types of Airports in India including Metros and Non-Metros for non-core security duties. They defined their role and suggested deployment patterns etc. along with cost savings thereof. The Government of India and the Airport Authority of India have taken up five points out of 22 points for implementation.

It is heartening to see that the IISSM's study has led to a change in the history of Aviation Security in India. Soon we will see that the airports (especially small ones) are fully functional without any operational and security challenges and economically viable. Implementation of the recommendations of the IISSM shows the quality of work that was performed by its Study Team and true to its reputation the IISSM has produced an outstanding study report that can be a benchmark for future such studies.

About the Author: Mr. Hiranya Mohanty is President in SIS (I) Private Limited, who was also the member of the study.

Mr.Hiranya Mohanty
President,
SIS (I) Private Limited
New Delhi

Role of the Private Security Industry in the Aviation Sector

Introduction.

The International Institute of Security and Safety Management (IISSM) is an ISO 9001:2015 Certified Centre of Excellence on Training in Security, Safety, and Loss Prevention. IISSM is a not-for-profit educational institute registered in 1992 under the Indian Societies Act. It is also registered with the Ministry of Micro, Small & Medium Enterprises, Government of India. IISSM is committed to promoting professionalism among security, safety, and fire prevention practitioners. Apart from conducting several training courses for security professionals, the IISSM offers consultancy services and conducts security and safety audits of hospitals, industrial complexes, banks, offices, etc.

IISSM conducted a nationwide consultancy project for the Ministry of Civil Aviation on the Role of the Private Security Industry in the Aviation Sector to reduce the cost of security at all airports in India. Their comprehensive study by a team of internationally recognized airport security experts that IISSM had put together found that several non-core security functions at our airports could be delegated to private security agencies having expertise in this area thus reducing the cost of airport security. These functions so far had been largely manned by state police forces and the CAPFs like the CISF. The study also showed that this approach could also release substantial numbers of government forces that are already over-stretched for other core duties.

The IISSM submitted its report to the Ministry of Civil Aviation in Oct 2019. The study team of IISSM comprised highly qualified professionals including internationally recognized Aviation Security Experts. The IISSM consulted all the stakeholders including AAI, BCAS, CISF, GMR, DIAL, BIAL, HIAL, and Air India, and took their inputs before finalizing the report. It also studied the best practices in civil aviation security followed in the USA, Canada, and Australia. The report had, inter alia, recommended that in line with best global AVSEC practices, 24 AVSEC security functions could be considered for categorizing as non-core, resulting in substantial savings in the cost of managing Airport Security.

Out of these 24 non-core functions recommended in the report by IISSM, MOCA has categorized the following 5 AVSEC functions as the main non-core functions:

- Segregation gate (Arrival/ Departure)
- Access Control/access denial
- Baggage controller / XBIS
- Access to visitor gallery and
- Security of vital installation

The above-mentioned 5 functions would go a long way in reducing the cost of managing security at our airports without in any way diluting the core security functions that can never be compromised.

The IISSM learnt that the AAI was keen to award these non-core functions to DGR registered Companies only. It felt that given the technological advancement in the environment, the need for a younger profile for the security workforce, and the fact that the security industry is a well-regulated industry that functions under the Private Security Agencies Regulation Act, 2005 (PSARA) and is considered an organized sector, that all PSAR Licence Service Providers should be permitted in executing the 5 non-core function, mentioned at Para (3) above. Accordingly, IISSM conveyed its views to the Ministry of Civil Aviation in Nov 2021 for their consideration.

With the managing of non-core functions by the Private Security Industry, the cost of Security at Airports will be reduced considerably and this cost reduction will certainly benefit the traveling public as fight fares and services at airports are expected to come down.

Conclusion. It is the considered opinion of aviation security domain experts and the civil aviation industry that more-and-more non-core functions of Aviation Security could be handled by introducing state-of-art-technology and more duties could be handed over to the Private Security Industry, thereby, further reducing the cost of Security Management at the Airports. The benefits that accrue will certainly be passed on to the passengers, thereby, reducing the cost of air travel in India.

Brig. A K Pathak (Retd.)
Deputy DG (Academics)
IISSM, New Dehi

IISSM

32nd IISSM ANNUAL GLOBAL CONCLAVE 18 - 19 NOVEMBER 2022

VIRTUAL CONCLAVE

IISSM ANNUAL GLOBAL CONCLAVE

ON

SECURITY, SAFETY AND LOSS PREVENTION : AN ENABLER FOR NATION BUILDING

SAVE THE DATE

18 - 19

FRIDAY SATURDAY

NOVEMBER, 2022

KEY NOTE TOPICS

- Role of Security, Safety and Loss Prevention in Nation Building.
- Technological Advancements and their application in Security, Safety and Loss Prevention Industry.
- National Critical Infrastructure in Cyberspace: Strategic Implications and Challenges.
- Technological Advances in Management of Smart Cities.

PANEL DISCUSSION TOPICS

- Role of Security, Safety and Loss Prevention in National Growth
- Technological Challenges in Security, Safety and Loss Prevention Industry.
- Cyber Security, Robotics and Drones in Security, Safety and Loss Prevention
- Management of Security, Safety and Loss Prevention in Smart Cities : Strengths, Weaknesses, Opportunities and Threats

Delegate Fee

Rs. 10,000.00 (GST Applicable)

helpdesk@iissm.com
www.iissm.com

Registration
099992 11650 # 95820 26101