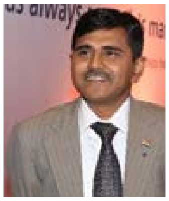
The oldest and one of the most prominent professional safety societies in the world.

ASSE-India Newsletter

Issue: February / 2018 **Issue number: ASSE INDIA - 48**

ASSE India – Newsletter Committee
Sandip Mukherjee

Message from the President's Desk....



February 26, 2018

Dear colleagues,
Greetings!

According to previous experiences, like every year, enhanced economic activities during the last leg of the fiscal year 2017 – 18 is anticipated. This means running towards achieving various targets, including production and productivity targets. This further gets accelerated with the end date approaching, sometimes with chaotic inputs, due to which probability of leaving serious scar just could get heightened. I sincerely believe that OSH professionals has a key role to play in this context to effectively facilitate handling of the emerging OSH challenges by the concerned line functionaries thereby protecting the people, property and the environment. I am sure each one of us would be striving to do our best towards that direction.

In India, 4th March is observed as National Safety Day. This is day when National Safety Council of India was established in 1972. I wish you all the very best for National Safety Day 2018.

ASSE India Chapter was established in Chennai on 4th March 2012 coinciding with National Safety Day celebrations. Hence, as we are gearing up for the celebration of 47th National Safety Day, we also get set for the observance of 6th annual day of ASSE India Chapter. However, as decided in our AGM subsequently, we would be celebrating this day a bit later, i.e., on 28th April 2018, coinciding with the "World Day for Safety and Health at Work".

Accordingly, 6th Professional Development Conference (PDC) of ASSE India Chapter has been scheduled to be held in Mumbai during 27-28 April 2018. I look forward to participation of you and your team in this event.

With best wishes and warm regards,

Krishna Nirmalya Sen, Ph.D, P.E., FIE
President
ASSE India Chapter

Content:

Editor's Corner:

Dear Reader,

We are presenting the 48th Issue of ASSE India Chapter Newsletter.

Now a days technology evolvements is guiding businesses through a data driven decision making process. Not only business, also in our personal life we use technology for storing all our data. So it is being increasingly felt to ensure security and safety of these data. Continuous effort is required for strengthening this security system. Furnishing an article on information security to enhance our understanding.

4th March is National Safety Day. Industries in India are celebrating National Safety Day / Week. Do send the information how you have celebrated this event in your work place. Also find some other important days those people are going to celebrate worldwide in this month.

Health is wealth. So read health tips on prevention of tuberculosis along with your favorite quiz contest.

Time is ticking for forthcoming ASSE India Chapter PDC. So rush to enhance your OSH knowledge and exposure from one of the best professional meet.

Do keep on sending interesting articles on OH&S for publication. Happy reading.

Warm Regards to all our Readers,
Sandip Mukherjee,
Chair – Newsletter (ASSE India Chapter)

Information Security

Information security, sometimes shortened to **InfoSec**, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take (e.g., electronic, physical). Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity. This is largely achieved through a multi-step risk management process that identifies assets, threat sources, vulnerabilities, potential impacts, and possible controls, followed by assessment of the effectiveness of the risk management plan.

To standardize this discipline, academics and professionals collaborate and seek to set basic guidance, policies, and industry standards on password, antivirus software, firewall, encryption software, legal liability and user/administrator training standards. This standardization may be further driven by a wide variety of laws and regulations that affect how data is accessed, processed, stored, and transferred. However, the implementation of any standards and guidance within an entity may have limited effect if a culture of continual improvement isn't adopted.

Overview

At the core of information security is information assurance, the act of maintaining the confidentiality, integrity and availability (CIA) of information, ensuring that information is not compromised in any way when critical issues arise. These issues include but are not limited to natural disasters, computer/server malfunction and physical theft. While paper-based business operations are still prevalent, requiring their own set of information security practices, enterprise digital initiatives are increasingly being emphasized, with information assurance now typically being dealt with by information technology (IT) security specialists. These specialists apply information security to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber-attacks that often attempt to acquire critical private information or gain control of the internal systems.

The field of information security has grown and evolved significantly in recent years. It offers many areas for specialization, including securing networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning, electronic record discovery, and digital forensics. Information security professionals are very stable in their employment. As of 2013 more than 80 percent of professionals had no change in employer or employment over a period of a year, and the number of professionals is projected to continuously grow more than 11 percent annually from 2014 to 2019.

Threats

Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile, are prone to theft and have also become far more desirable as the amount of data capacity increases. Sabotage usually consists of the destruction of an organization’s website in an attempt to cause loss of confidence on the part of its customers. Information extortion consists of theft of a company’s property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner, as with ransomware. There are many ways to help protect you from some of these attacks but one of the most functional precautions is user carefulness.

Governments, military, corporations, financial institutions, hospitals and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, as well as damage to the company's reputation. From a business perspective, information security must be balanced against cost; the Gordon-Loeb Model provides a mathematical economic approach for addressing this concern.

For the individual, information security has a significant effect on privacy, which is viewed very differently in various cultures.

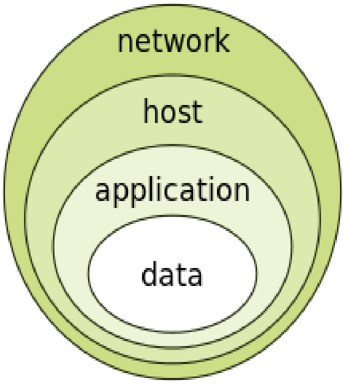
Responses to threats

Possible responses to a security threat or risk are –

- **reduce/mitigate** – implement safeguards and countermeasures to eliminate vulnerabilities or block threats
- **assign/transfer** – place the cost of the threat onto another entity or organization such as purchasing insurance or outsourcing
- **accept** – evaluate if the cost of the countermeasure outweighs the possible cost of loss due to the threat

Risk Management

The *Certified Information Systems Auditor (CISA) Review Manual 2006* provides the following definition of risk management: "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.



There are two things in this definition that may need some clarification. First, the *process* of risk management is an ongoing, iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerabilities emerge every day. Second, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Risk analysis and risk evaluation processes have their limitations since, when security incidents occur, they emerge in a context, and their rarity and uniqueness give rise to unpredictable threats. The analysis of these phenomena, which are characterized by breakdowns, surprises and side-effects, requires a theoretical approach that is able to examine and interpret subjectively the detail of each incident.

Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). Vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (man-made or act of nature) that has the potential to cause harm.

The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called "residual risk."

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis.

Research has shown that the most vulnerable point in most information systems is the human user, operator, designer, or other human. The ISO/IEC 27002:2005 Code of practice for information security management recommends the following be examined during a risk assessment:

- security policy,
- organization of information security,
- asset management,
- human resources security,
- physical and environmental security,
- communications and operations management,
- access control,
- information systems acquisition, development and maintenance,
- information security incident management,
- business continuity management, and
- regulatory compliance.

In broad terms, the risk management process consists of:

1. Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, and other), and supplies.
2. Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, and malicious acts originating from inside or outside the organization.
3. Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.
4. Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.
5. Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.
6. Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernible loss of productivity.

For any given risk, management can choose to accept the risk based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business. Or, leadership may choose to mitigate the risk by selecting and implementing appropriate control measures to reduce the risk. In some cases, the risk can be transferred to another business by buying insurance or outsourcing to another business. The reality of some risks may be disputed. In such cases leadership may choose to deny the risk.

Security controls

Selecting and implementing proper security controls will initially help an organization bring down risk to acceptable levels. Control selection should follow and should be based on the risk assessment. Controls can vary in nature, but fundamentally they are ways of protecting the confidentiality, integrity or availability of information. ISO/IEC 27001 has defined controls in different areas. Organizations can implement additional controls according to requirement of the organization. ISO/IEC 27002 offers a guideline for organizational information security standards.

Administrative

Administrative controls consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day-to-day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed – the Payment Card Industry Data Security Standard (PCI DSS) required by Visa and MasterCard is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls, which are of paramount importance.

Logical

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. Passwords, network and host-based firewalls, network intrusion detection systems, access control lists, and data encryption are examples of logical controls.

An important logical control that is frequently overlooked is the principle of least privilege, which requires that an individual, program or system process not be granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read email and surf the web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change, employees are promoted to a new position, or employees are transferred to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges, which may no longer be necessary or appropriate.

Physical

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities and include doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and workplace into functional areas are also physical controls.

An important physical control that is frequently overlooked is separation of duties, which ensures that an individual cannot complete a critical task by himself. For example, an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator; these roles and responsibilities must be separated from one another.

Process

The terms "reasonable and prudent person," "due care" and "due diligence" have been used in the fields of finance, securities, and law for many years. In recent years these terms have found their way into the fields of computing and information security. U.S. Federal Sentencing Guidelines now make it possible to hold corporate officers liable for failing to exercise due care and due diligence in the management of their information systems.

In the business world, stockholders, customers, business partners and governments have the expectation that corporate officers will run the business in accordance with accepted business practices and in compliance with laws and other regulatory requirements. This is often described as the "reasonable and prudent person" rule. A prudent person takes due care to ensure that everything necessary is done to operate the business by sound business principles and in a legal ethical manner. A prudent person is also diligent (mindful, attentive, and ongoing) in their due care of the business.

Security governance

The Software Engineering Institute at Carnegie Mellon University, in a publication titled *Governing for Enterprise Security (GES) Implementation Guide*, defines characteristics of effective security governance. These include:

- An enterprise-wide issue
- Leaders are accountable
- Viewed as a business requirement
- Risk-based
- Roles, responsibilities, and segregation of duties defined
- Addressed and enforced in policy
- Adequate resources committed
- Staff aware and trained
- A development life cycle requirement
- Planned, managed, measurable, and measured
- Reviewed and audited

Incident Response Plans

An incident response plan that addresses how discovered breaches in security are also vital. It should include:

- Selection of team members
- Definition of roles, responsibilities and lines of authority
- Definition of a security incident
- Definition of a reportable incident
- Training
- Detection
- Classification
- Escalation
- Containment
- Eradication
- Documentation

Change management

Change management is a formal process for directing and controlling alterations to the information processing environment. This includes alterations to desktop computers, the network, servers and software. The objectives of change management are to reduce the risks posed by changes to the information processing environment and improve the stability and reliability of the processing environment as changes are made. It is not the objective of change management to prevent or hinder necessary changes from being implemented.

Any change to the information processing environment introduces an element of risk. Even apparently simple changes can have unexpected effects. One of management's many responsibilities is the management of risk. Change management is a tool for managing the risks introduced by changes to the information processing environment. Part of the change management process ensures that changes are not implemented at inopportune times when they may disrupt critical business processes or interfere with other changes being implemented.

Not every change needs to be managed. Some kinds of changes are a part of the everyday routine of information processing and adhere to a predefined procedure, which reduces the overall level of risk to the processing environment. Creating a new user account or deploying a new desktop computer is examples of changes that do not generally require change management. However, relocating user file shares, or upgrading the Email server pose a much higher level of risk to the processing environment and are not a normal everyday activity. The critical first steps in change management are (a) defining change (and communicating that definition) and (b) defining the scope of the change system.

Change management is usually overseen by a change review board composed of representatives from key business areas, security, networking, systems administrators, database administration, application developers, desktop support and the help desk. The tasks of the change review board can be facilitated with the use of automated work flow application. The responsibility of the change review board is to ensure the organization's documented change management procedures are followed. The change management process is as follows –

Request: Anyone can request a change. The person making the change request may or may not be the same person that performs the analysis or implements the change. When a request for change is received, it may undergo a preliminary review to determine if the requested change is compatible with the organizations business model and practices, and to determine the amount of resources needed to implement the change.

Approve: Management runs the business and controls the allocation of resources therefore; management must approve requests for changes and assign a priority for every change. Management might choose to reject a change request if the change is not compatible with the business model, industry standards or best practices. Management might also choose to reject a change request if the change requires more resources than can be allocated for the change.

Plan: Planning a change involves discovering the scope and impact of the proposed change; analyzing the complexity of the change; allocation of resources and, developing, testing and documenting both implementation and back-out plans. Need to define the criteria on which a decision to back out will be made.

Test: Every change must be tested in a safe test environment, which closely reflects the actual production environment, before the change is applied to the production environment. The back out plan must also be tested.

Schedule: Part of the change review board's responsibility is to assist in the scheduling of changes by reviewing the proposed implementation date for potential conflicts with other scheduled changes or critical business activities.

Communicate: Once a change has been scheduled it must be communicated. The communication is to give others the opportunity to remind the change review board about other changes or critical business activities that might have been overlooked when scheduling the change. The communication also serves to make the help desk and users aware that a change is about to occur. Another responsibility of the change review board is to ensure that scheduled changes have been properly communicated to those who will be affected by the change or otherwise have an interest in the change.

Implement: At the appointed date and time, the changes must be implemented. Part of the planning process was to develop an implementation plan, testing plan and, a back out plan. If the implementation of the change should fail or, the post implementation testing fails or, other "drop dead" criteria have been met, the back out plan should be implemented.

Document: All changes must be documented. The documentation includes the initial request for change, its approval, the priority assigned to it, the implementation, testing and back out plans, the results of the change review board critique, the date/time the change was implemented, who implemented it, and whether the change was implemented successfully, failed or postponed.

Post-change review: The change review board should hold a post-implementation review of changes. It is particularly important to review failed and backed out changes. The review board should try to understand the problems that were encountered, and look for areas for improvement.

Change management procedures that are simple to follow and easy to use can greatly reduce the overall risks created when changes are made to the information processing environment. Good change management procedures improve the overall quality and success of changes as they are implemented. This is accomplished through planning, peer review, documentation and communication.

Business Continuity

Business continuity management (BCM) concerns arrangements aiming to protect an organization's critical business functions from interruption due to incidents, or at least minimize the effects. BCM is essential to any organization to keep technology and business in line with current threats to the continuation of business as usual. The BCM should be included in an organizations risk analysis plan to ensure that all of the necessary business functions have what they need to keep going in the event of any type of threat to any business function.

It encompasses:

- Analysis of requirements, e.g., identifying critical business functions, dependencies and potential failure points, potential threats and hence incidents or risks of concern to the organization;
- Specification, e.g., maximum tolerable outage periods; recovery point objectives (maximum acceptable periods of data loss);
- Architecture and design, e.g., an appropriate combination of approaches including resilience (e.g. engineering IT systems and processes for high availability, avoiding or preventing situations that might interrupt the business), incident and emergency management (e.g., evacuating premises, calling the emergency services, triage/situation assessment and invoking recovery plans), recovery (e.g., rebuilding) and contingency management (generic capabilities to deal positively with whatever occurs using whatever resources are available);
- Implementation, e.g., configuring and scheduling backups, data transfers, etc., duplicating and strengthening critical elements; contracting with service and equipment suppliers;
- Testing, e.g., business continuity exercises of various types, costs and assurance levels;
- Management, e.g., defining strategies, setting objectives and goals; planning and directing the work; allocating funds, people and other resources; prioritization relative to other activities; team building, leadership, control, motivation and coordination with other business functions and activities (e.g., IT, facilities, human resources, risk management, information risk and security, operations); monitoring the situation, checking and updating the arrangements when things change; maturing the approach through continuous improvement, learning and appropriate investment;
- Assurance, e.g., testing against specified requirements; measuring, analyzing and reporting key parameters; conducting additional tests, reviews and audits for greater confidence that the arrangements will go to plan if invoked.

Whereas BCM takes a broad approach to minimizing disaster-related risks by reducing the probability and the severity of incidents, a disaster recovery plan (DRP) focuses specifically on resuming business operations as quickly as possible after a disaster. A disaster recovery plan, invoked soon after a disaster occurs, lays out the steps necessary to recover critical information and communications technology (ICT) infrastructure. Disaster recovery planning includes establishing a planning group, performing risk assessment, establishing priorities, developing recovery strategies, preparing inventories and documentation of the plan, developing verification criteria and procedure, and lastly implementing the plan.

Information Security Culture

Employee behavior can have a big impact on information security in organizations. Cultural concepts can help different segments of the organization work effectively or work against effectiveness towards information security within an organization. "Exploring the Relationship between Organizational Culture and Information Security Culture" provides the following definition of information security culture: "ISC is the totality of patterns of behavior in an organization that contribute to the protection of information of all kinds."

Andersson and Reimers (2014) found that employees often do not see themselves as part of the organization Information Security "effort" and often take actions that ignore organizational information security best interests. Research shows information security culture needs to be improved continuously. In *Information Security Culture from Analysis to Change*, authors commented, "It's a never ending process, a cycle of evaluation and change or maintenance." To manage the information security culture, five steps should be taken: pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation.

- Pre-Evaluation: to identify the awareness of information security within employees and to analysis current security policy
- Strategic Planning: to come up a better awareness-program, we need to set clear targets. Clustering people is helpful to achieve it
- Operative Planning: create a good security culture based on internal communication, management buy-in, security awareness and training programs
- Implementation: should feature commitment of management, communication with organizational members, courses for all organizational members, and commitment of the employees
- Post-evaluation: to better gauge the effectiveness of the prior steps and build on continuous improvement

Sources and Standards

The International Organization for Standardization (ISO) is a consortium of national standards institutes from 157 countries, coordinated through a secretariat in Geneva, Switzerland. ISO is the world's largest developer of standards. ISO 15443: "Information technology – Security techniques – A framework for IT security assurance", ISO/IEC 27002: "Information technology – Security techniques – Code of practice for information security management", ISO-20000: "Information technology – Service management", and ISO/IEC 27001: "Information technology – Security techniques – Information security management systems – Requirements" are of particular interest to information security professionals.

The US National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. The NIST Computer Security Division develops standards, metrics, tests and validation programs as well as publishes standards and guidelines to increase secure IT planning, implementation, management and operation. NIST is also the custodian of the U.S. Federal Information Processing Standard publications (FIPS).

The Internet Society is a professional membership society with more than 100 organizations and over 20,000 individual members in over 180 countries. It provides leadership in addressing issues that confront the future of the internet and is the organizational home for the groups responsible for internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). The ISOC hosts the Requests for Comments (RFCs) which includes the Official Internet Protocol Standards and the RFC-2196 Site Security Handbook.

The Information Security Forum is a global nonprofit organization of several hundred leading organizations in financial services, manufacturing, telecommunications, consumer goods, government, and other areas. It undertakes research into information security practices and offers advice in its biannual Standard of Good Practice and more detailed advisories for members.

The Institute of Information Security Professionals (IISP) is an independent, non-profit body governed by its members, with the principal objective of advancing the professionalism of information security practitioners and thereby the professionalism of the industry as a whole. The institute developed the IISP Skills Framework. This framework describes the range of competencies expected of information security and information assurance professionals in the effective performance of their roles. It was developed through collaboration between both private and public sector organizations and world-renowned academics and security leaders.

The German Federal Office for Information Security (in German *Bundesamt für Sicherheit in der Informationstechnik (BSI)*) BSI-Standards 100-1 to 100-4 are a set of recommendations including "methods, processes, procedures, approaches and measures relating to information security". The BSI-Standard 100-2 *IT-Grundschutz Methodology*describes how information security management can be implemented and operated. The standard includes a very specific guide, the IT Baseline Protection Catalogs (also known as IT-Grundschutz Catalogs). Before 2005, the catalogs were formerly known as "IT Baseline Protection Manual". The Catalogs are a collection of documents useful for detecting and combating security-relevant weak points in the IT environment (IT cluster). The collection encompasses as of September 2013 over 4,400 pages with the introduction and catalogs. The IT-Grundschutz approach is aligned with to the ISO/IEC 2700x family.

Source: https://en.wikipedia.org

Important days in Safety, Health and Environmental Calendar of March, 2018

World Wildlife Day 03 March 2018

On 20 December 2013, at its 68th session, the United Nations General Assembly (UNGA) proclaimed 3 March, the day of signature of the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), as UN World Wildlife Day to celebrate and raise awareness of the world's wild animals and plants. The UNGA resolution also designated the CITES Secretariat as the facilitator for the global observance of this special day for wildlife on the UN calendar. World Wildlife Day has now become the most important global annual event dedicated to wildlife.

World Wildlife Day will be celebrated in 2018 under the theme **"Big cats: predators under threat".**

Big cats are among the most widely recognized and admired animals across the globe. However, today these charismatic predators are facing many and varied threats, which are mostly caused by human activities. Overall, their populations are declining at a disturbing rate due to loss of habitat and prey, conflicts with people, poaching and illegal trade. For example, tiger populations plummeted by 95% over the past 100 years and African lion populations dropped by 40% in just 20 years. But a range of measures are underway to arrest this decline.

In an effort to reach as wide an audience as possible, the expanded definition of big cats is being used, which includes not only lion, tiger, leopard and jaguar -- the 4 largest wild cats that can roar - but also cheetah, snow leopard, puma, clouded leopard, etc. Big cat species are found in Africa, Asia, and North, Central and South America, representing a virtually global distribution, and representations of big cats, such as for car logos, by sporting clubs and the fashion industry, are used globally.

Over the past century we have been losing big cats, the planet's most majestic predators, at an alarming rate. World Wildlife Day 2018 gives us the opportunity to raise awareness about their plight and to galvanize support for the many global and national actions that are underway to save these iconic species. Through World Wildlife Day big cats will generate the level of attention they all deserve to be sure they are with us for generations to come."

In line with the UN General Assembly Resolution proclaiming World Wildlife Day, the CITES Secretariat calls on all member States and organizations of the United Nations system and other global, regional and sub-regional organizations, non-governmental organizations and all interested individuals, to: observe and raise awareness of the theme for World Wildlife Day 2018 in an appropriate manner; to associate the celebrations with major national and international conservation events, where appropriate; to organize campaigns to reduce the demand for illegal wildlife and their products using targeted strategies in order to influence consumer behavior; and to make use of the World Wildlife Day logo as widely as possible.

Governments, law makers, enforcement officers, customs officials and park rangers across every region are scaling up their efforts to protect wildlife. It is also up to every citizen, young and old, to protect wildlife and their habitats. We all have a role to play. Our collective conservation actions can be the difference between a species surviving or disappearing.

Source: http://www.wildlifeday.org

National Safety Day 04th March 2018

The National Safety Day/Week Campaign is celebrated in India every year (organized by the National Safety Council) to commemorate the establishment of this event, 4th of March as well as enhance the safety awareness among people. National Safety Council of India is a self-governing body (nonprofit and nongovernmental organization for public service) which was established on 4th of March in 1966 under the Societies Act in Mumbai, having over 8000 members. It is a national movement carried out on annual basis to prevent and lessen the loss of life including various human being problems and their financial loss through availing them with safety, health and environment related support services.

It is celebrated with great enthusiasm to make aware the people about how to get prevented from the industrial accidents by exhibiting widespread safety awareness programs in the public sectors which have not been covered by any safety legislation. During whole week campaign celebration, varieties of specific activities are displayed to the people as per the safety requirements.

National Safety Day / Week Celebration

It is celebrated by uniting together the governmental and nongovernmental organizations including the health organizations and industrial members. They are well supplied with all the centrally designed promotional materials and utilities (badge, stickers, banners, instruction card, poster, wallet, leather belt and bag) printed with SHE slogans and messages by the Council to fulfill the following objectives:

- For the convenience of the campaign organizing organizational members.
- For making sure about the quality materials which should reflect the national SHE issues.
- For generating support to the organizations in order to contribute to the economic self-reliance of the National Safety Council.

In order to organize this campaign, a national level and safe governmental support is given to the members. The campaign is well planned to make it highly visible among the people through the efficient use of an electronic media journals, newspapers and other industrial magazines.

Following national level activities for whole week such as variety of public functions including seminars, debates, poster of safety messages and slogans distribution, essay competitions, safety awards distribution, banner exhibition, play of drama and songs, training programs, workshops, display of films over SHE issues are held during the campaign celebration. Safety Pledge event is carried out by the organizational employees.

Safety activities based training programs are held for the industrial staffs over various topics to carry out their responsibilities very well. During training session they are taught about the testing and examination of pressure vessels, lifting machines, chemical and electrical safety, risk handling and assessment, fire control, first aid knowledge and etc.

Objectives of Celebrating National Safety Day / Week

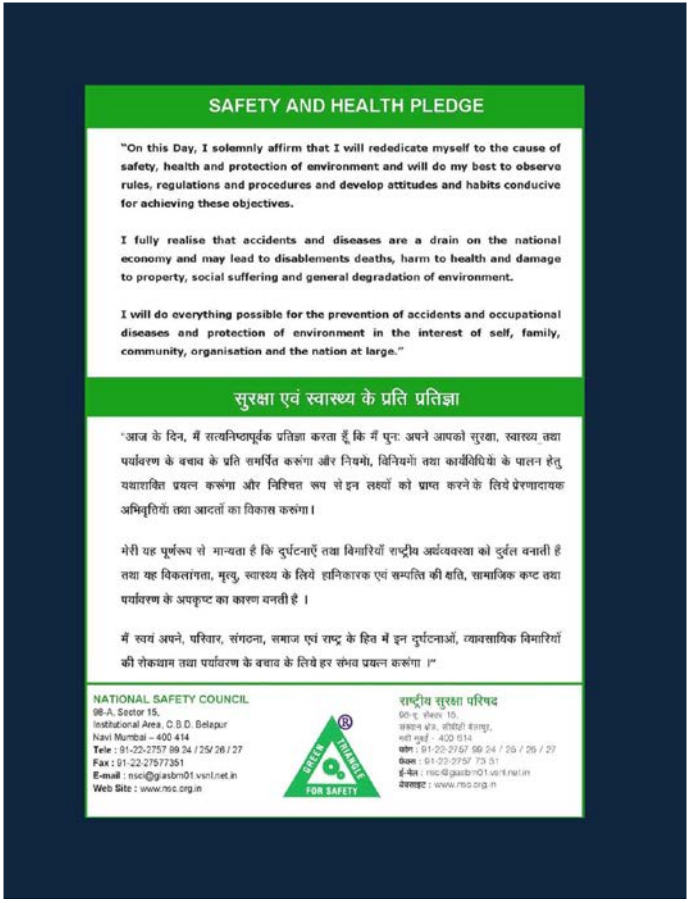
- National Safety Day/Week is celebrated on national level all over the country to aware people about safety including the various health and environmental movements.
- It is celebrated to get the goal of great level of the public participation to play the major safety roles in different industrial sectors.
- Through the campaign celebration it is largely promoted the utilization of participative approach by the owners of the company by promoting their staffs in the safety, health and environmental activities.
- Through this campaign, the need-based activities, self-observance with legal requisites and professional SHE (safety, health and environmental) activities are encouraged among staffs at the work places.
- Work place safety is promoted to a great level by reminding the employers and employees including other staffs of their legal responsibilities.
- To get the goal of developing and strengthening the SHE activities among people to the workplaces.
- Serve the society with preventive culture and scientific state of mind by organizing a safety approach.

Activities at Enterprise Level

- Administration of Safety Pledge by the employees. The model text of the Safety Pledge designed, developed and distributed by the NSC.
- Unfurling of the NSD Flag.
- Pinning of the NSD badge on employees.
- Banners displayed at strategic locations in the units.
- Safety competitions - Essay, Slogans, Posters, Housekeeping, Safety Performance, etc.
- Safety suggestions.
- Exhibitions.
- One-act play/drama, songs, quawalis.
- Training Programs/Workshops/Seminars, etc.
- Screening of safety films in units/employee colonies.
- Practical demonstrations on PPE/Fire Fighting, etc.
- Organizing emergency drills.

- Display of Mobile Exhibition.
- Holding award functions.
- Invite eminent guest speakers.
- Community Awareness Programs.

Safety Pledge Published by National Safety Council



SAFETY AND HEALTH PLEDGE

"On this Day, I solemnly affirm that I will rededicate myself to the cause of safety, health and protection of environment and will do my best to observe rules, regulations and procedures and develop attitudes and habits conducive for achieving these objectives.

I fully realise that accidents and diseases are a drain on the national economy and may lead to disablements deaths, harm to health and damage to property, social suffering and general degradation of environment.

I will do everything possible for the prevention of accidents and occupational diseases and protection of environment in the interest of self, family, community, organisation and the nation at large."

सुरक्षा एवं स्वास्थ्य के प्रति प्रतिज्ञा

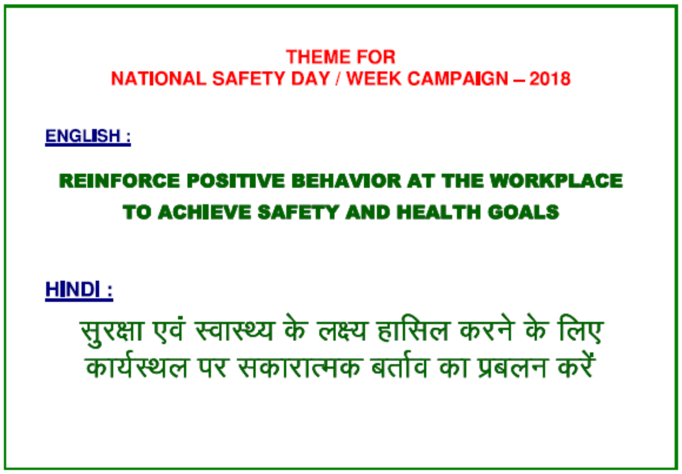
"आज के दिन, मैं सत्यनिष्ठापूर्वक प्रतिज्ञा करता हूँ कि मैं पुनः अपने आपको सुरक्षा, स्वास्थ्य तथा पर्यावरण के बचाव के प्रति समर्पित करूंगा और नियमों, विनियमों तथा कार्यविधियों के पालन हेतु यथाशक्ति प्रयत्न करूंगा और निश्चित रूप से इन लक्ष्यों को प्राप्त करने के लिये प्रेरणादायक अभिवृत्तियों तथा आदतों का विकास करूंगा।

मेरी यह पूर्णरूप से मान्यता है कि दुर्घटनाएँ तथा बिमारियाँ राष्ट्रीय अर्थव्यवस्था को दुर्बल बनाती हैं तथा यह विकलांगता, मृत्यु, स्वास्थ्य के लिये हानिकारक एवं सम्पत्ति की क्षति, सामाजिक कष्ट तथा पर्यावरण के अपकृष्ट का कारण बनती हैं ।

मैं स्वयं अपने, परिवार, संगठना, समाज एवं राष्ट्र के हित में इन दुर्घटनाओं, व्यावसायिक बिमारियों की रोकथाम तथा पर्यावरण के बचाव के लिये हर संभव प्रयत्न करूंगा ।"

NATIONAL SAFETY COUNCIL
98-A, Sector 15,
Institutional Area, C.B.D. Belapur
Navi Mumbai – 400 414
Tele : 91-22-2757 99 24 / 25/ 26 / 27
Fax : 91-22-27577351
E-mail : nsci@giasbm01.vsnl.net.in
Web Site : www.nsc.org.in

राष्ट्रीय सुरक्षा परिषद
98-ए, सेक्टर 15,
संस्थान क्षेत्र, सीबीडी बेलापुर,
नवी मुंबई - 400 614
फोन : 91-22-2757 99 24 / 25 / 26 / 27
फैक्स : 91-22-2757 75 51
ई-मेल : nsci@giasbm01.vsnl.net.in
वेबसाइट : www.nsc.org.in



THEME FOR
NATIONAL SAFETY DAY / WEEK CAMPAIGN – 2018

ENGLISH :

REINFORCE POSITIVE BEHAVIOR AT THE WORKPLACE
TO ACHIEVE SAFETY AND HEALTH GOALS

HINDI :

सुरक्षा एवं स्वास्थ्य के लक्ष्य हासिल करने के लिए
कार्यस्थल पर सकारात्मक बर्ताव का प्रबलन करें

Source: http://www.indiacelebrating.com; http://nsc.org.in

International Woman's Day 08 March 2018

The theme for International Women's Day, 8 March, is **"Time is Now: Rural and urban activists transforming women's lives".**

This year, International Women's Day comes on the heels of unprecedented global movement for women's rights, equality and justice. Sexual harassment, violence and discrimination against women has captured headlines and public discourse, propelled by a rising determination for change.

People around the world are mobilizing for a future that is more equal. This has taken the form of global marches and campaigns, including #MeToo in the United States of America and its counterparts in other countries, protesting against sexual harassment and violence, such as #YoTambien in Mexico, Spain, South America and beyond, #QuellaVoltaChe in Italy, #BalanceTonPorc in France and #Ana_kaman in the Arab States; "Ni Una Menos" ('not one less'), a campaign against femicide that originated in Argentina; and many others, on issues ranging from equal pay to women's political representation.

International Women's Day 2018 is an opportunity to transform this momentum into action, to empower women in all settings, rural and urban, and celebrate the activists who are working relentlessly to claim women's rights and realize their full potential.

Echoing the priority theme of the upcoming 62nd session of the UN Commission on the Status of Women, International Women's Day will also draw attention to the rights and activism of rural women, who make up over a quarter of the world population and majority of the 43 per cent of women in the global agricultural labor force.

They till the lands and plant seeds to feed nations ensure food security for their communities and build climate resilience. Yet, on almost every measure of development, because of deep seated gender inequalities and discrimination, rural women fare worse than rural men or urban women. For instance, less than 20 per cent of landholders worldwide are women, and while the global pay gap between men and women stand at 23 per cent, in rural areas, it can be as high as 40 per cent. They lack infrastructure and services, decent work and social protection, and are left more vulnerable to the effects of climate change.

Making the promise of the Sustainable Development Goals a reality, to *leave no one behind,* needs urgent action in rural areas to ensure an adequate standard of living, a life free of violence and harmful practices for rural women, as well as their access to land and productive assets, food security and nutrition, decent work, education and health, including their sexual and reproductive health and rights.

Rural women and their organizations represent an enormous potential, and they are on the move to claim their rights and improve their livelihoods and wellbeing. They are using innovative agricultural methods, setting up successful businesses and acquiring new skills, pursuing their legal entitlements and running for office. Recently, as hundreds of courageous women from the film, theatre and art industry in the USA started speaking against sexual harassment and assault by powerful men in the industry, they found a powerful ally in Alianza Nacional de Campesinas, the national farmworker women's organization, no stranger to the abuse of power.

On 8 March, join activists around the world and UN Women to seize the moment, celebrate, take action and transform women's lives everywhere. The time is NOW.

Source: http://www.unwomen.org

World Tuberculosis Day 24 March 2018

World Tuberculosis Day is a worldwide event that aims to raise public awareness of tuberculosis and the efforts made to prevent and treat this disease. This event is held on March 24 each year and is promoted by organizations such as the World Health Organization (WHO).

What Do People Do?

Various World Tuberculosis Day events and activities are organized by various organizations involved in the Stop TB Partnership. WHO is a United Nations' (UN) health authority that works with this network to promote World Tuberculosis Day each year. Campaign activities include:

- Community discussion groups that are organized to look at ways to prevent TB.
- Award ceremonies or other events to honor the life and work of those who dedicate their lives to prevent and fight against TB.
- Photo exhibitions that showcase images to raise worldwide awareness of TB.
- Charity events to raise funds for disease control (of TB) in countries that need assistance.

People, community groups and government agencies may also take the time to work with broadcast, print and online media to promote stories on the awareness of tuberculosis and the works of those who help fight against the spread of the disease.

Background

Tuberculosis, or TB, is an infectious bacterial disease caused by Mycobacterium tuberculosis, which most commonly affects the lungs. It is transmitted from person to person via droplets from the throat and lungs of people with the disease. WHO estimates that the largest number of new TB cases in 2005 occurred in south-east Asia, which accounted for 34 percent of incident cases globally. However, the estimated incidence rate in sub-Saharan Africa is nearly twice that of south-east Asia.

World Tuberculosis Day, annually held on March 24, marks the day in 1882 when Dr Robert Koch detected the cause of tuberculosis, the TB bacillus. This was a first step towards diagnosing and curing tuberculosis. World Tuberculosis Day can be traced back to 1982, when the International Union against Tuberculosis and Lung Disease launched World TB Day on March 24 that year, to coincide with the 100th anniversary of Dr Koch's discovery.

In 1996, the World Health Organization (WHO) joined the union and other organizations to promote World TB Day. The Stop TB Partnership, called the Stop TB Initiative at the time of its inception, was established in 1998. It is a network of organizations and countries fighting tuberculosis. WHO works with this partnership on to support the activities and events that take place on World Tuberculosis Day each year.

Source: http://www.timeanddate.com

Health Tips

Tuberculosis (TB) Prevention – Vaccine, drug treatment and isolation

Strategies for TB Prevention

TB prevention consists of several main parts. The first part of TB prevention is to stop the transmission of TB from one adult to another. This is done through firstly, identifying people with active TB, and then curing them through the provision of drug treatment.

With proper TB treatment someone with TB will very quickly not be infectious and so can no longer spread the disease to others. The second main part of TB prevention is to prevent people with latent TB from developing active, and infectious, TB disease.

Anything which increases the number of people infected by each infectious person, such as ineffective treatment because of drug resistant TB, reduces the overall effect of the main TB prevention efforts. The presence of TB and HIV infection together also increases the number of people infected by each infectious person. As a result it is then more likely that globally the number of people developing active TB will increase rather than decrease.

The third part of TB prevention is TB infection control. This means preventing the transmission of TB in such settings as hospitals & prisons.

The pasteurization of milk also helps to prevent humans from getting bovine TB.

There is a vaccine for TB, but it makes only a small contribution to TB prevention. It does little to interrupt the transmission of TB among adults.

TB prevention – the BCG vaccine

The vaccine called Bacillus Calmette-Guerin (BCG) was first developed in the 1920s. It is one of the most widely used of all current vaccines, and it reaches more than 80% of all new born children and infants in countries where it is part of the national childhood immunization programme.[1] However, it is also one of the most variable vaccines in routine use.

The BCG vaccine has been shown to provide children with excellent protection against the disseminated forms of TB. However protection against pulmonary TB in adults is variable. Since most transmission originates from adult cases of pulmonary TB, the BCG vaccine is generally used to protect children, rather than to interrupt transmission among adults.

The BCG vaccine will often result in the person vaccinated having a positive result to a TB skin test.

TB education

TB education is necessary for people with TB. People with TB need to know how to take their TB drugs properly. They also need to know how to make sure that they do not pass TB on to other people. But TB education is also necessary for the general public. The public needs to know basic information about TB for a number of reasons including reducing the stigma still associated with TB.

TB Treatment as TB prevention

TB drug treatment for the prevention of TB, also known as chemoprophylaxis, can reduce the risk of a first episode of active TB occurring in people with latent TB. The treatment of latent TB is being used as a tool to try and eliminate TB in the United States.

Isoniazid is one of the drugs used to prevent latent TB from progressing to active TB or TB disease. Isoniazid is a cheap drug, but in a similar way to the use of the BCG vaccine, it is mainly used to protect individuals rather than to interrupt transmission between adults. This is because children rarely have infectious TB, and it is hard to administer isoniazid on a large scale to adults who do not have any symptoms. Taking isoniazid daily for six months is difficult in respect of adherence, and as a result many individuals who could benefit from the treatment, stop taking the drug before the end of the six month period.

There have also been concerns about the possible impact of TB treatment for prevention programs on the emergence of drug resistance. However, a review of the scientific evidence has now shown that there is no need for this to be a concern. The benefit of isoniazid preventative therapy for people living with HIV, and who have, or may have had latent TB, has also recently been emphasized.

Preventing TB transmission in households

Actions to be taken

In order to reduce exposure in households where someone has infectious TB, the following actions should be taken whenever possible:

- Houses should be adequately ventilated;
- Anyone who coughs should be educated on cough etiquette and respiratory hygiene, and should follow such practice at all times;
- While smear positive, TB patients should:
  - Spend as much time as possible outdoors;
  - If possible, sleep alone in a separate, adequately ventilated room;
  - Spend as little time as possible on public transport;
  - Spend as little time as possible in places where large numbers of people gather together.

Cough etiquette and respiratory hygiene means covering your nose and mouth when coughing or sneezing. This can be done with a tissue, or if the person doesn't have a tissue they can cough or sneeze into their upper sleeve or elbow, but they should not cough or sneeze into their hands. The tissue should then be safely disposed of.[3] Educating people about TB is also an important part of TB prevention, as well as ensuring that people who need TB treatment receive it as soon as possible.

Households where someone has culture positive MDR TB

It is not fully known how differences between drug susceptible, and drug resistant TB, as well as HIV status, affect the risk of TB transmission. However it is thought that people with drug resistant TB remain infectious for much longer, even if treatment has been started, and this may prolong the risk of transmission in the household.

In households with culture positive MDR TB patients, the following guidance should therefore be observed in addition to the measures given above.

- Culture positive MDR TB patients who cough should always practice cough etiquette (including use of masks) and respiratory hygiene when in contact with people. Ideally health service providers should wear respirators when attending patients with infectious MDR TB in enclosed spaces.;
- Ideally, family members living with HIV, or family members with strong clinical evidence of HIV infection, should not provide care for patients with culture positive MDR TB;
- Children below five years of age should spend as little time as possible in the same living spaces as culture positive MDR TB patients.

Face masks are different from respirators and can be made from either cloth or paper. A face mask worn by someone with infectious TB can help to prevent the spread of M. tuberculosis from the patient to other people. The face mask can capture large wet particles near the mouth and nose of the patient, preventing the bacteria from being released into the environment. Cloth masks can be sterilized and reused.

Respirators can protect health care workers from inhaling M. tuberculosis in certain circumstances, but they are expensive to purchase and they require specialized equipment to ensure that they fit properly. The use of a face mask does not protect health care workers against TB, and so a health care worker or other staff should not wear a face mask in a household (or indeed in a health care) setting.

Households where someone has XDR TB

If some has culture positive XDR TB, then they should be isolated at all times, and any person in contact with a culture positive XDR TB patient should wear a particulate respirator. If at all possible, HIV positive family members, or family members with strong clinical evidence of HIV infection, should not share a household with a culture positive XDR TB patient.

Physical measures for TB prevention

Before drug treatment for TB became available, removing TB patients from their homes and putting them in isolation in sanatoria, was the main way of reducing the transmission of TB.

However this policy changed in the vast majority of countries, after studies showed that if patients stayed at home and were treated on an “outpatient” basis, this did not increase the risk of TB amongst the household contacts of the people with TB. This is because drug treatment quickly makes a TB patient un-infectious, and most household contacts who do become infected, will have already become infected before the diagnosis of TB has been made.

So generally there is now no need for people to leave their homes because they have TB. The only exception to this is, as described above, when someone has infectious XDR TB, and it is not feasible to isolate them at home. Also people may still need to go into a health care facility because there are complications arising from their condition, or their treatment. Within a health care facility there may be a need for some separation of people in order to reduce the chances of transmission.

The measures described above also mainly apply to resource poor settings, and the recommendations can be different where more resources are available.

TB prevention in health care facilities

Doctors and other health care workers, who provide care for patients for TB, must follow infection control procedures to ensure that TB infection is not passed from one person to another. Every country should have infection control guidance which clearly needs to take into account local facilities and resources, as well as the number of people being provided with care. However, infection control guidance must not only be written but also implemented.

Source: **http://www.tbfacts.org**

Information on forthcoming events

20th CONGRESS
INTERNATIONAL ERGONOMICS ASSOCIATION
FLORENCE August 26th-30th, 2018

The Italian Society of Ergonomics is pleased to host in 2018 in Florence, the 20th international IEA conference. It is the first time in the history of the 50 years of the IEA and the SIE that this event will take place in Italy. The theme of the congress is “Creativity in Practice”, with reference to the typical challenge of the Italian way to innovation. **Students from middle and low income countries (whose Abstracts are accepted) will get their registration for free and their accommodation for free.**

Website: http://iea2018.org/
Important dates:
12th February 2018 Notification for accepted Abstracts

30th April 2018 Deadline for Early Bird registrations, and submission of extended papers

SAFETY 2018
ASSE
ASSE PROFESSIONAL DEVELOPMENT
CONFERENCE & EXPOSITION
Exposition: June 3-5, 2018
Conference: June 3-6, 2018
safety.asse.org
San Antonio

ASSE Region IX (Global) Professional Development Webinar Series #3

Innovative Environmental Technologies- A Safer and Faster Vitrification for Oil Spills

March 29, 2018

11.00 CST

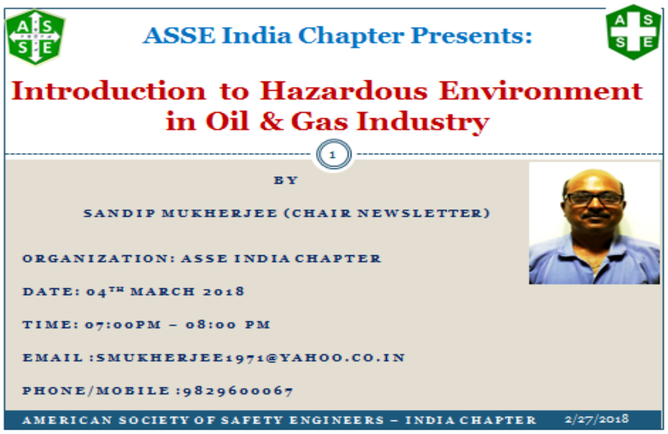
Speakers: **Mr. Rupal S. Amin, Ph.D. and Mr. Stephen Lancaster**

Register Now

After registering, you will receive a confirmation email containing information about joining the webinar.

For more information on the webinar, please contact Region IX Professional Development Chair, Mr. Daniel Osadiaye at danielosadiaye@yahoo.com or Ashok Garlapati, CSP,CFIOSH,QEP, Region IX RVP at ashokcpcl@yahoo.com.

Forthcoming ASSE India Chapter’s Webinar Information


ASSE India Chapter Presents:

Introduction to Hazardous Environment in Oil & Gas Industry

1

BY

SANDIP MUKHERJEE (CHAIR NEWSLETTER)

ORGANIZATION: ASSE INDIA CHAPTER

DATE: 04TH MARCH 2018

TIME: 07:00PM – 08:00 PM

EMAIL :SMUKHERJEE1971@YAHOO.CO.IN

PHONE/MOBILE :9829600067

AMERICAN SOCIETY OF SAFETY ENGINEERS – INDIA CHAPTER 2/27/2018

Please register for Webinar on:

Introduction to Hazardous Environment in Oil & Gas Industry

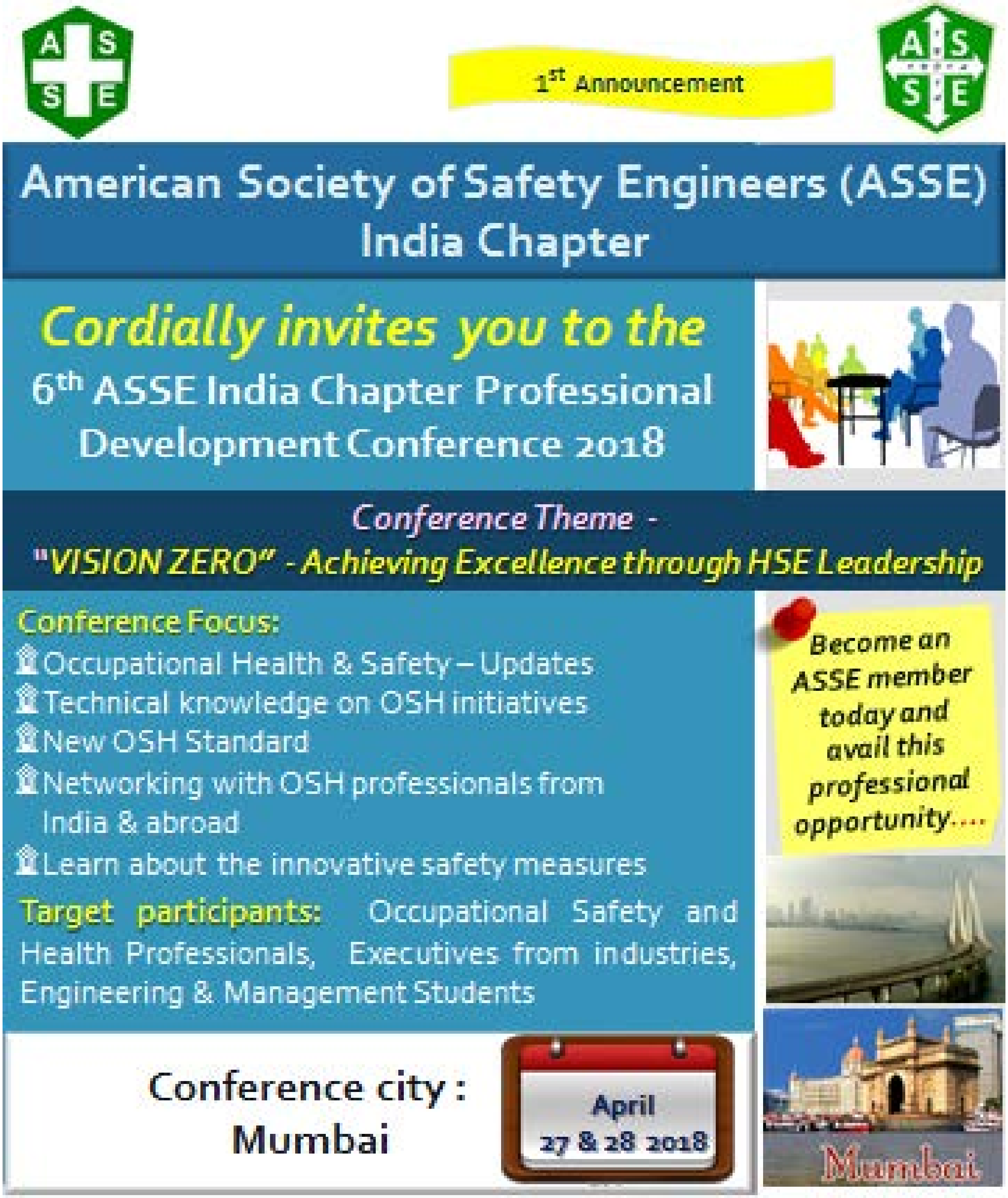
Scheduled on Mar 4, 2018 7:00 PM IST at:

https://attendee.gotowebinar.com/register/3387485763064718593

This webinar is delivered by Mr. Sandip Mukherjee, a veteran safety professional in Oil & Gas field. Apart from his regular assignments he has been volunteering as Chair Newsletter of ASSE India Chapter for several years.

After registering, you will receive a confirmation email containing information about joining the webinar.

6th ASSE India Chapter Professional Development Conference 2018



1st Announcement

American Society of Safety Engineers (ASSE) India Chapter

Cordially invites you to the

6th ASSE India Chapter Professional Development Conference 2018

Conference Theme -

"VISION ZERO" - Achieving Excellence through HSE Leadership

Conference Focus:

- Occupational Health & Safety – Updates
- Technical knowledge on OSH initiatives
- New OSH Standard
- Networking with OSH professionals from India & abroad
- Learn about the innovative safety measures

Target participants: Occupational Safety and Health Professionals, Executives from industries, Engineering & Management Students

Become an ASSE member today and avail this professional opportunity....

Conference city : Mumbai

April
27 & 28 2018

1st Announcement

Annual Professional Development Conference of ASSE India Chapter is a 2 day (27th & 28th April'18) event featuring rich content shared by eminent expert professionals from respective fields on various topics:

- Managing OSH in Large Projects
- Ergonomics
- OSH Challenges in manufacturing sector
- Application of emerging technologies in OSH
- OSH in Commercial Establishments
- Legal frameworks on safety
- Road Safety

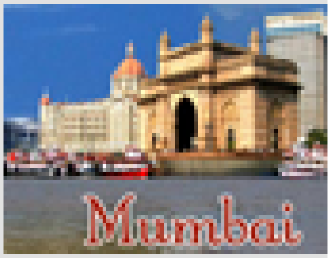
Professional net working and updates on the subjects…

Registration is free for speakers. A nominal registration charge for the participants may be assigned which will be notified to the interested individuals in advance.

For registration write to Mr V. Janardhanam, Secretary ASSE India Chapter and Joint Secretary ASSE India Chapter PDC 2018

EMAIL : vjana05@gmail.com

Mentioning participants name, designation, organization, contact details etc.



Opportunities:

- Presentation of paper by experienced professionals from industry and academia
- Presentation by budding safety professionals
- Registration will cover participation in both days including lunch tea etc.
- Selected paper may be recommended for publication in ASSE Journal/ Newsletter

Brochure

ASSE - INDIA CHAPTER
PROTECTING PEOPLE, PROPERTY and the ENVIRONMENT

HSE Quiz

1. What is the key to effective safety management?

A Engineering control of workplace hazards
B Safety committee
C Establishing accountability
D Compliance with industry standard

2. Profit that is not distributed among shareholders or owners is:

A Called retained earnings
B Called business equity
C Called excess profit
D Retained assets for research and development

3. **Which of the following is the first step in establishing an effective process safety management program?**

A Written process safety management program
B Employee training
C Hazard analysis
D Establishing the safety culture

4. The boom indicator on a mobile crane:

A Shows the safe load at any boom angle
B Provide the angle of the boom
C Signals when the crane is out of balance
D Indicate lifting capacity

5. Which radioactive emission is the easiest one to shield against?

A Alpha
B Beta
C X-ray
D Gamma

Watch out the next issue for correct answer

Answers from last issue's (January / 2018) Quiz: 1 (D); 2 (C); 3 (B); 4 (C); 5 (A)

You are welcome to send your inputs to: Sandip Mukherjee; e-mail: newsletter@india.asse.org; Phone: +91 9829600067

Selected articles shall be published in next publication

Become an ASSE member today & avail a world of professional opportunities….

ASSE offers its members many opportunities for networking, professional development, global media outreach, government affairs programs, standards development, publications and other resources**. For further details, please contact:**

Mr. K. N Sen, President; email: krishnanirmalya@gmail.com; Phone - +91 9444399208

Mr. V Janardhanam, Secretary; email: vjana05@gmail.com ; Phone: +91 9500079757

For more information please visit our website - http://india.asse.org

Disclaimer: Every effort has been made to ensure the accuracy of the information contained in this newsletter. Still in case of any errors, ASSE- India Chapter or any members of the Chapter accepts no responsibility. The details given here are just for information and the reader should check it correctness from his/her resources and should not act on the basis of the information provided herein.