SECURITY INDIA

CARD 2015

COVERT SECURITY INDIA'S ANNUAL RISK DOSSIER

SECURITY INDIA

We wish the New Year brings you peace, success and good fortune!!

*As the new year begins so does a new chapter in the lives of the team at **Security India**. While being a new entrant in the Indian Security Consulting Industry, the stakeholders come along carrying a vast experience in providing quality services to clients across various industries having global repute.*

***Security India**, thus announces its arrival to the corporate stage and is happy to be connected with your organization and you!!*

www.security-india.com @security_india +91 97428 51208

Bengaluru I Hyderabad I Pune I NCR

Preface

Understanding of Security Risks is an integral part of today's business environment. A resilient organization not only needs to be focussing it's energies on strategic goals, but also needs to bridge all security risk gaps. The challenge however is to ensure provisioning of adequate resources, knowledge and capabilities to undertake a focused effort to understand and mitigate the persistent business risks.

Security India helps organizations understand and bridge gaps in order to de-risk businesses and help them meet their business objectives. With a large plethora of security vulnerabilities in the daily world, a specialist like **Security India** is required to qualify, quantify, document, report, communicate and provide de-risking strategies to all clients alike.

CARD - 2015 is a representation of business critical risks as identified by Security India that are expected to have maximum impact during the next six months. The risks have been compiled based on strategic analysis of organisations belonging to different sectors and geographical displacements in India. Our team at Security India is grateful to all our well wishers who most willingly accommodated us to facilitate a study and analysis of the same.

CARD - 2015 comprises of the following -

- Employee safety training
- Supply chain and logistics
- Geo-strategic competition risks
- Cyber risks
- Fire hazards
- Infrastructural risks
- Pandemic outbreaks

CARD - 2015

ECURITY INDIA

Employee Safety Training

Introduction

In a highly competitive global arena, organizations vie for numerous opportunities wherein they may display their prowess as well as their capabilities as a whole, to be the best business enhancers and solution providers. However, while their focus on organizational growth and achieving set goals and objectives, may be a requirement based on sustenance to say the least, protecting their vital people assets is an absolute necessity.

So, are we saying that employee safety is being neglected? While institutionally, an organization has numerous controls in place and incorporates the very best known industrial solutions to mitigate threats, the question is who verifies the following –

- Is there an existent standard operating procedure(SOP)or organizational process to keep check?
- What is the level of procedural implementations? Are these being audited / vetted?
- And most importantly, what is the level of safety awareness of an employee? How do we test their awareness? Are there any assessment parameters?

Challenges

While organizations are not really known to compromise on important aspects such as employee safety, what really differs in the final decision making step are factors intrinsic and extrinsic to the system. These factors bear a substantial impact on the implementation of robust safety systems. While the list of challenges is exhaustive, we have only focused upon the key areas of impact in this note.

Intrinsic factors include aspects as –

- Organizational risk appetite
- Enhancement of existent control measures and
- Implementation of industry best practices

Extrinsic factors include aspects as -

- Employee attrition (nearly 30%)
- Dependability on outsourced services
- Matching employee expectations.

Why are Efforts to Improve Safety Flat-lining?

If you look at a typical workplace safety program, it generally consists of 4 key elements:

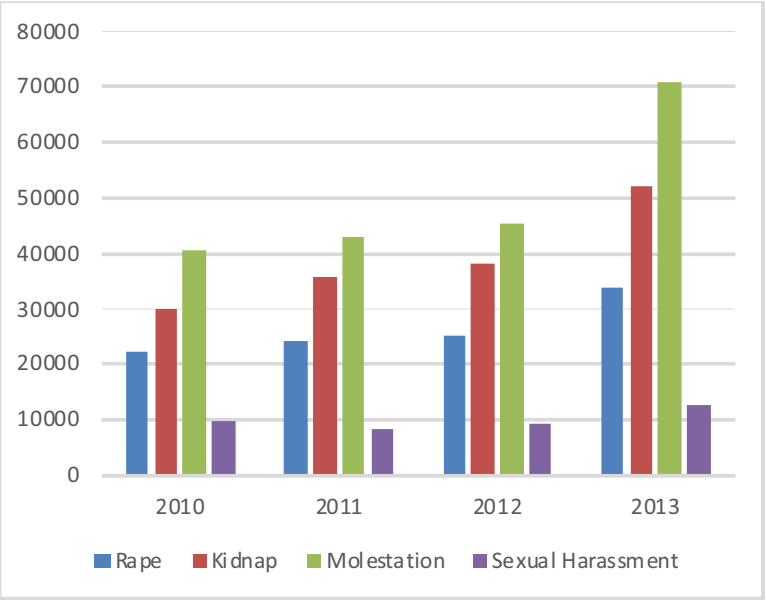
The Environment – How can both the physical and social environment be changed to make the workplace as safe as possible?
Policy – What policies or procedures are needed to help ensure manufacturing practices and processes are aligned with safety objectives?
Awareness - What level of awareness must employees maintain about safety on a day-to-day basis?
Training – What do people need to know, believe and do to improve workplace safety?

The limitation however lies in the fact that these workplace safety programs do not effectively identify and mitigate threat associated to personnel safety that are eventually being compromised. With organizations often turning a blind eye to such risks and even more to their employees after office hours, questions are raised on important issues such as when does the liability of an organization cease towards its employees. Working trends and life style changes lead to the over exposure of employees towards unwarranted situations that further lead to increasing anti-social crimes.

Key areas of concern for employee safety include –

- Transport safety – reliability of outsourced service provider and staff on duty
- Lack of safety awareness and adherence to safety norms by employees
- Lack of institutional methods and training aids to highlight key areas and aspects
- Anticipated requirement of heavy capital investment by management
- Lack of a holistic employee centric safety and security mechanism / program

While institutionally, numerous safe-guards have been factored within as well as catered for, the lack of their coverage and resultant effectiveness



have been questionable and thought provoking. Personnel crime statistics reveal alarming outcomes and the same increase when highlighting women safety in specific. A look at the following chart highlights the same.

Solutions

Organizations thus need to streamline their policies, processes and efforts towards imparting awareness and training at grass root levels not just as an obligation but with a focussed objective. The same can be achieved through dedicated training and interactive sessions. Third party vendors exhibiting expertise in the field may also be consulted.

CARD - 2015

ECURITY INDIA

Supply Chain Risks

Introduction

A supply chain stretches from the consignor to the consignee through nodes and links that are integral and unique to each one. This means the transport network is only the physical aspect that integrates into the supply chain. Several overlapping supply chains maybe functional at the same place and time in a business network.

Every Supply chain is defined based on its vulnerability to disruption in the supply chain process. This vulnerability is often due to unwanted effects caused either by internal or external forces that create disturbances larger than the supply chain is designed to handle.

As supply chains spread throughout the organization, even small disruptions can have large impacts on customer satisfaction and may pose a hindrance in meeting the organizations overall objectives. Organizations thus require supply chain risk assessment & security to prevent and protect against hostile threats that may affect the supply chain's continuity.

Current Issues and Challenges

In a rapidly growing and competitive industrial segment, supply chains are rightly perceived to be the game changers. Every impact on the chain may result in phenomenal and irreversible changes from a client perspective towards the organization. The challenges thus faced by the organization may be identified as under –

Complexity – From a systems perspective, transport and logistics involve material and goods, infrastructure and resources, information and the monetary elements moving in a complex unison. The flow of materials is the reason for the Supply Chain's existence but, it is only one part of the Supply Chain system. The second part is the flow of the flexible resources such as heavy duty trucks, trains, aeroplanes and ships which are required for the movement of the material through various infrastructural means such as roads, harbours, airports and terminals. These two parts represent the 'physical' part of logistics and are

supported by the monetary stream and the flow of information to complete the chain. The integration of these often pose a critical challenge as most managers hold *expertise in two to three* of the fields and have a short sightedness towards the fourth.

Reliance on external infrastructure - Transportation and logistics need geographically fixed constructions and infrastructure. Some of the infrastructure is owned and used exclusively by one company while some is co-owned or owned by governments due to economic, political and strategic impacts. This lack of control adds to uncertainty in the supply chain.

Globalization and Outsourcing – The scope and geographic coverage of Supply Chains has increased manifold in the past few decades due to modernization and globalization. As organizations become more focused, tasks redundant to the main strategy are often outsourced and thus make for further loose ends. This demands further diligence to manage the increased uncertainty. The possibility of failure may however be reduced to a large extent through stringent SOPs and good process controls.

Dynamic business environment – The anecdote - "change is the only constant" - has never been as true as it is now. With shrinking time lines, focus on reliable delivery schedules and competitive environment - awareness, information and adaptability are more important than ever.

Threats to supply chains

Crime – Crime has the ability to disrupt and even disable a supply chain. But, it is nearly impossible for a company to foresee and mitigate the risk. Managing crime requires not just local escorts and protection personnel but also the support of local law enforcement agencies and political bodies. Adequate planning, routine training and a good foresight can help mitigate against nearly 95% of all crimes.

Considering factors such as available statistics, local area maps and country or area specific risk ratings can help in creating a good foresight.

Shrinkage and Theft – 'Inventory shrinkage' refers to the loss of products between the point of manufacturing or purchase and the point of sale.

Four major sources of shrinkage are:

- Employee theft
- Shoplifting
- Administrative error
- Vendor fraud

The first three sources can be overcome through dedicated effort, diligent process controls and constant monitoring. However, vendor fraud is an area that is highly sensitive and requires critical assessments and routine auditing to ensure its viability and acceptability.

Shrinkage during distribution / transportation is approximately 0.14 percent of annual sales for all types of products, while the worldwide loss ratio is pinned around 0.025 percent of the total revenue. Audits can reveal such loop holes in the system and provide information to strengthen the supply chain.

Terrorism – It is one of the major obstacles for international business. It requires meaningful international countermeasures to understand and manage. Business in areas with known threats from terrorism must be carefully considered and vetted for opportunities.

Terrorist attacks around the world have clearly indicated that logistic operations are the one that always suffer the consequences. There thus lies a question of whether such attacks can have a negative impact on productivity or by warranting higher costs for more secure transactions, higher insurance premiums, and counterterrorism efforts, the attacks may be mitgated.

Dependency on Insurance – While having your consignments insured is a good practice as it helps protect you against the various risks and transit losses, dependency on the same often lands organizations into trouble. While an insurance reimburses you monetarily, it does not help you in the following critical aspects–

- Retaining customers that impatiently turn to other suppliers during a crisis; and rarely return
- In replacing loss of both people and equipment assets
- Protecting your brand reputation.

Way ahead

Based on the numerous challenges posed by a supply chain process, organizations are relying on greater support from in-house as well as industry experts to protect them from the risks. Some of these viable options include –

- Gaining timely alerts and advice based on the alerts to allow for quick decision making
- Conduct of third party audits to identify and plug gaps in the system
- Create channels for flow of information through the supply chain according to the business environment and needs
- Manage supply chain channels on a customised platform suited to each area of operation
- Plans may be based on site investigation and / or business intelligence enquiries and further audits as required.

CARD - 2015

Geostrategic Competition Risk

Introduction

With technological advancements and growing economies, all organizations aim for greater success based on their organizational goals, their services and products offered as well as their leadership position in their particular area of operations. However, irrespective of their overall goals and objectives, all organizations are associated with each other on a common platform, that being monetary success. It is the demand of higher revenues on year-on-year basis that primarily associate with and drive the Geo-strategic Competition Risk.

A deeper thought on the subject leaves us with the debate on whether such competition is considered to be healthy or not. The decision to be made is left to your organizations and you. To assist you with the same, a few vital risks associated and their mitigations have been highlighted in this document.

Challenges

Best known organizations are driven by sound planning, advanced industry knowledge and delivery capabilities. Yet, time and again, decisions made for organizational benefits can result in otherwise adverse results. Key identified challenges in the industry include –

- Competitors – A common requirement of clients, allowing multiple vendors to possess compliance capability
- Timelines – Stringent delivery timelines across industries
- Sub-contracting – Wide project scope that leads to necessitating of outsourcing;
- Attrition – High attrition rates of employees, especially skilled workforce
- Brand protection

Decision Making

The above challenges pose numerous constraints and demand unique requirements and responses from the management and employees alike. However, factors that may primarily influence the decision making under those circumstance are –

- Low management risk appetite
- Short sightedness in anticipating competitor responses
- Lack of a holistic project based delivery capability

- Lack of systematic training, monitoring and enhancement of career opportunities especially of skilled workforce
- Reliability of outsourcing – including meeting of quality and delivery standard requirements

Based on these factors, the organization is often forced to accept risks and take strategic decisions with an expectation of payoff. Unfortunately, when these decisions back fire, the organizations are both directly and in-directly impacted.

A typical example of what Geo-strategic competition risk can do to your organization can be derived from the numerous automobile recalls from some of the top-globally recognised brands for minor faults. Though the intention there was to protect the brand as a whole, the bypassing of laid down norms and poor planning of risks forced them to dilute their brand.

Solutions

Though there is no definite or clear path that would assure a 100% mitigation, incorporation of the succeeding vital aspects into the organizational policy would help build value and strengthen the brand as a whole. The aspects include but are not restricted to –

- Focus on employee assets
- High standard of delivery
- Observing lifestyle trends and conducting routine checks on employees
- Conduct of vendor specific due-diligence
- Maintaining high valued work culture and ethics
- Building brand loyalty equally amongst employees, vendors and clients alike
- Ensuring achievement of long term goals versus short-term gains

Road Ahead

The road map ahead is clear. Yet, it will continue to test the risk appetites, growth strategies and competitiveness of all industries alike. Taking decisions will get more and more critical as newer players would regularly enter the market with competing benefits and advantages.

The much sought after, first mover advantage too would continue to drive organizations ahead with stringent timelines and hard to achieve targets so as to gain an overall competitive advantage over compatriots in the field. However, all of it would once again highlight the challenges that we have already discussed thus far. Thus, the critical question that one needs to ask themselves is –

What has more value to me as an organization? Brand, Money or Service Quality.

Cyber Risks

Introduction

Cyber security involves people, processes and technologies. With technology advancing at a never seen before pace, organizations are increasingly getting dependent and are neglecting the people assets and processes in the bargain which thereby enhances their cyber security risks. In the year 2014, virtually every industrial sector has been affected by some type or variant of cyber threat.

Moreover, it is rare that organizations have the right practitioners, tools and executive leadership required to understand and respond to security challenges. Businesses that have security awareness report significantly lower average financial losses from cyber security incidents.

Another key area of cyber risks is that of cloud computing which is rapidly becoming a key component of many organisations' technology enablement strategies as they continue to seek differentiation in competitive markets. Cloud however is a significant issue from a risk perspective, both in the context of governance and compliance, for example, geographic location of data – are you sure where personnel data is resident and is that consistent with the jurisdiction of geographies where client organisations operate?

A worldwide survey by Kaspersky Lab and B2B International resulted in indicating that 93% of financial services organizations experienced various cyber threats in the period between April 2013 and May 2014.

Cyber Risks

Organizations are forced to accept cyber risks as a part of their daily operations. In the current day scenario, the primary areas which threaten organizations are –

Employees – They are considered to be the weakest part of any data security program. Employees regularly fall victim to increasingly-sophisticated phishing and spear-phishing emails. Clicking an enticing link often covertly loads malware that provides a hacker entry into your system. The silver lining is that organizations have more control over

their employees than the other actors in a data security event (viz. hackers/vendors)

Vendors – They cause or contribute to nearly half of all data breaches. Despite this, organizations often overlook the threat posed by vendors and ignore vendor due diligence. Furthermore, if we consider our employees as one of the greatest threats to cyber risks, vendor's employees are further out of direct control, while their actions can expose our sensitive data easily. Nearly 15% of incidents in the previous year can be attributed to current and former service providers, consultants and contractors.

Corporate culture – Recognizing that the threat actors are not going away, corporate culture is at the heart of the cyber risk problem for the senior management. While they shape the culture, the "who we are" of an organization they also ask are we security conscious? Do we think that data security is an "IT issue" or do we acknowledge that it is only a prerogative of the management alone? If budgets reflect an organization's priorities, what is your data security budget?

Data security thus needs to be an integral part of the corporate culture. Its incorporation facilitates the involvement of an individual for security; time and money are allocated to train employees, manage vendors and to set up layered security (e.g. data classification and data segmentation, user access controls, encryption); regular risk assessments identify and address vulnerabilities; incident response plans are created and tested; and the board of directors involved insist up on implementing data security best practices.

Current Trend

While risk has become universal, financial losses due to security incidents vary widely based on the organizational size. Large companies typically spend more on information security and have a more mature program. Larger organizations also take a more strategic approach to security by identifying sensitive assets and allocating spending to their most valuable data. They are also likely to understand third-party risks through the use of security baselines for

partners and act upon the importance of employee training.

Mitigation Strategies

We need to remember, that our cyber risk transfer solutions must be needs led and not product led. Options commonly used in the industry to mitigate risks include –

Vendor Protection – To ensure that they have the ability to safeguard the information, have robust contractual protection and conduct ongoing monitoring to ensure that the third party is protecting the data.

Cyber Insurance – Policies have been developed by insurers to help businesses and individuals protect themselves from the cyber threat. Market intelligence suggests that the types of specialized cyber coverage being offered by insurers are expanding in response to this fast-growing market need.

Testing of available software tools – Numerous tools available in the market are often subjected to various cyber risks. Hence proper testing / vetting is recommended. Avoiding over dependency is also mandated as they tend to provide temporary solutions and not a composite fool proof protection.

Knowledge up-gradation & training – Effective security will require knowledge about existing and potential adversaries, including their motives, resources and methods of attack. This will not happen without a budget for threat analysis and monitoring, as well as a commitment of time and resources coupled with periodic training.

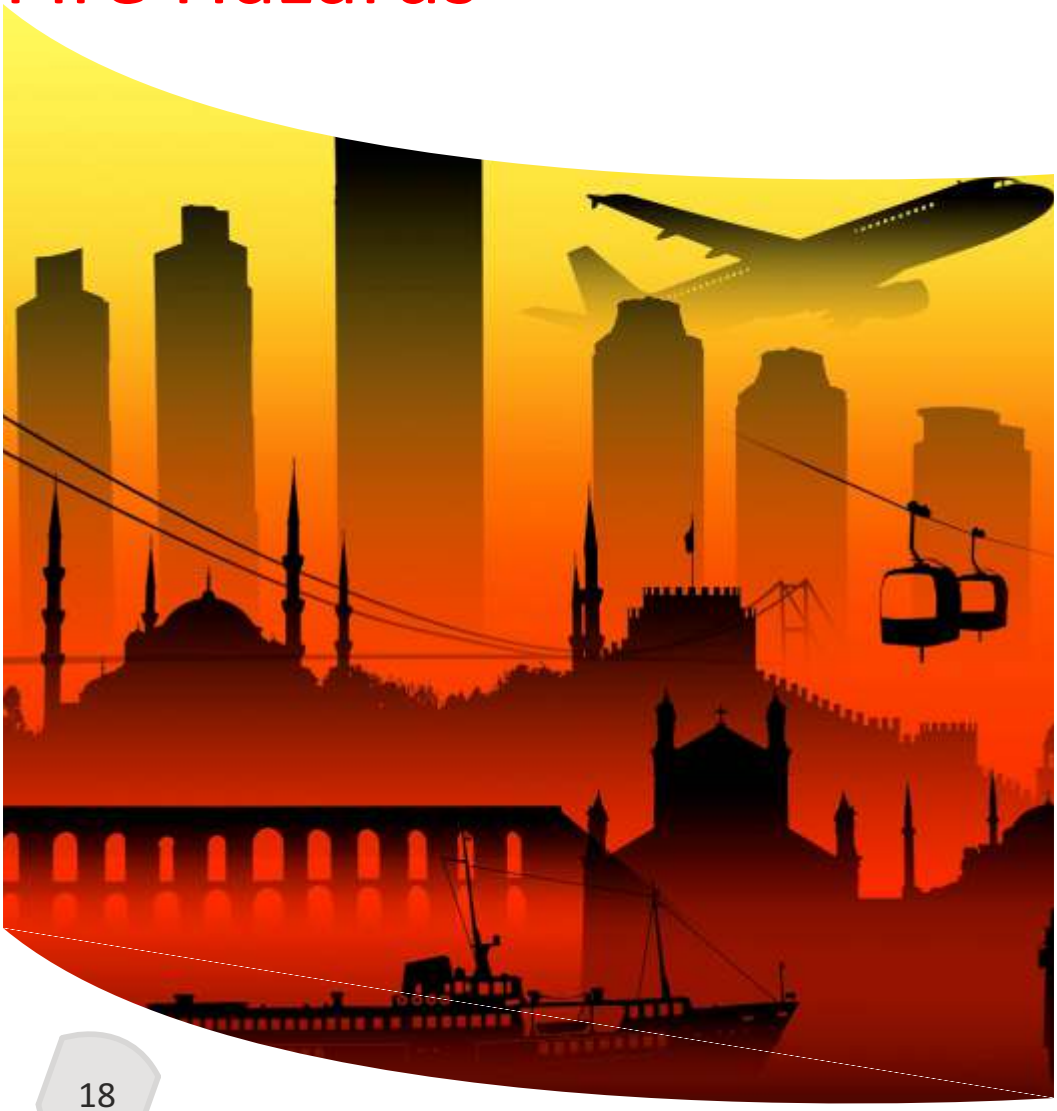
Looking Ahead

The techniques, tactics and procedures used to date are still considered to be in the nascent stage of targeting the financial system and other critical infrastructures. There however persists an ever increasing threat that cyber breaches could penetrate core systems and disrupt crucial operational functions. Thus sooner, organizations identify and respond to developing situations, its mitigation would be easier and the associated losses could be minimised.

CARD - 2015

ECURITY INDIA

Fire Hazards



Introduction

Businesses, organizations and industries are subject to risks alike that are often attributable to unchecked and preventable hazards. Hazards and accidents may be classified under man-made and natural. Man-made hazards are often easily identifiable and can be mitigated with necessary precautions. Natural hazards and accidents on the other hand require a higher level of awareness and diligence to be addressed. Needless to say, these hazard risks are preferred to be transferred.

Amongst all types of hazards, in India, fire has been the single most detrimental industrial risk. Nearly 40% of all industrial accidents caused over the last three years were attributed towards fire.

The main causes of fire are primarily electrical causes (like short-circuiting, over-loading and tapping of supply for alternate lines) and incidents caused due to negligence and non-compliance of laid down precautions.

Impact of Industrial Accidents

Economic impact is obvious in the case of industrial accidents but not limited to it. Brand perception is significantly compromised when the cause of the accident is negligence on the part of the organization. Employees subjected to undue risk may be demoralized. Economic losses may be recovered relatively easily compared to brand perception.

When industrial accidents are considered, the Bhopal gas tragedy is the first to come to mind. Though many norms and standards have been developed and adopted since, the Indian subcontinent has witnessed numerous devastating accidents, some of which of recent times are highlighted below.

01 Feb 2015 – Dhaka, Bangladesh

At Least 13 employees died and dozens others were injured in a fire that swept through a plastic packaging factory. The cause of the fire was attributed to a faulty gas cylinder and a boiler unit.

30 Jan 2015 – Vellore, Tamil Nadu

10 employees belonging to a tannery died due to polluting effluents that swamped an area meant only for dry sludge. The incident was attributed to non-compliance of regulatory norms as well as poor maintenance of the tannery.

The factory had been operating without appropriate permits and inadequate safety measures. No fire safety devices were installed and the workspaces were cramped leaving no room for the employees to escape.

20 October 2014 – Hyderabad, Telangana

17 employees lost their lives and more than 30 others were injured due to an explosion in a fireworks factory in Andhra Pradesh.

Causes and Prevention of Industrial Accidents

Standards and regulations for the prevention of industrial accidents have seen numerous improved versions since the 1960s. Whether we talk about the Bureau of Indian Standards (BIS), the National Building codes (NBC), the Occupational Safety and Health Administration (OSHA) or any other standard, organizations have failed to upgrade themselves as well the knowledge of their employees. With rapid industrialization and a greater focus on monetary gains, precautions and implementations concerning fire hazard risks, continue losing their necessary importance and due care.

Way Forward

Organizations have to perforce lay greater emphasis, ensure conduct of regular third party audits to identify lapses and potential hazardous situations and diligently train 100% of their employees on its identification and mitigation. This would not only ensure sustainability, but also be a leading factor in the growth of the organization.

Pandemic Outbreak

Introduction

A pandemic is a global disease outbreak. It is determined by how the disease spreads and not by how many deaths it causes. When a new influenza virus emerges, a flu pandemic can occur. Because the virus is new, the human population often has little to no immunity against it. The virus spreads quickly from person-to-person worldwide.

Contemporary pandemics and outbreaks of disease, such as the current H1N1 influenza (Swine Flu) pandemic, Ebola, as well as the emergence of H5N1 influenza (Avian Flu) virus and severe acute respiratory syndrome (SARS)-associated coronavirus, serve as poignant reminders of our global vulnerability to emergent threats to human health and our current inability to predict or prevent such events.

However, despite the seemingly unpredictable nature of disease emergence, there are lessons to be learned from the origins of these diseases, lessons that may offer clues as to how future infectious disease outbreaks and pandemics may occur and more importantly be prevented. The challenge lies in using the accumulated, albeit incomplete, knowledge gained from emergent diseases of our past to identify practical solutions and strategies aimed at detecting and halting future threats.

Challenges

For organizations operating across diverse segments and facing widespread geographical displacement, the biggest challenge is to meet the operational requirements during pandemic outbreaks that can virtually have a paralyzing effect. The challenges of a pandemic outbreak include–

- Rapid worldwide spread
- Overloaded health care systems
- Inadequate medical supplies
- Lack of infrastructure to facilitate treatment
- Disrupted economy and society

Mitigation Strategies

Most mitigation strategies require the involvement of global resources and government bodies to formulate

and implement the same. In the absence of these stakeholders, organizations are expected to resort to local resources in an attempt to meet the basic requirements and to implement the basic processes and procedures. The following strategies may be adopted at local organizational levels.

- Reduce human exposure to the virus – by educating employees on its nature and effects.
- Strengthen the early warning system and have plans ready to either mitigate or to deal with situation once it develops
- Restrict movement of employees to affected regions to an on necessity basis; travel need not be cancelled. It may be delayed or postponed.
- Ensure that affected regions have availability of all data and clinical specimens needed for an accurate risk assessment and for speedy treatment in case diagnosed
- Prepare in-house teams to take charge where possible or have tie-ups with local medical agencies for aided support

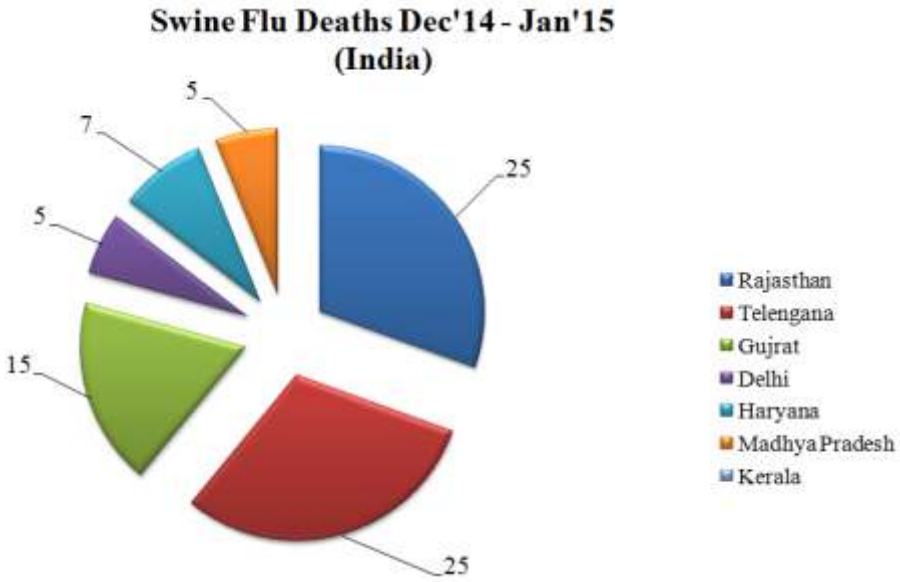
Advantageous actions that may be taken at governmental levels include –

- Training of personnel for intensifying rapid containment operations – For preventing the virus from further increasing its transmissibility among humans or delay its international spread
- Build capacity to cope with a pandemic – Ensure that all countries have formulated and tested pandemic response plans and that a central agency like the WHO is in complete control and able to perform its leadership role during a pandemic
- Co-ordinate global scientific research and development – Ensure that pandemic vaccines and anti-viral drugs are rapidly and widely available shortly after the start of a pandemic and that scientific understanding of the virus evolve quickly

- Capacity building for medical evacuations / isolations – Identification and demarcation of areas having capabilities to cater to larger volumes of individuals

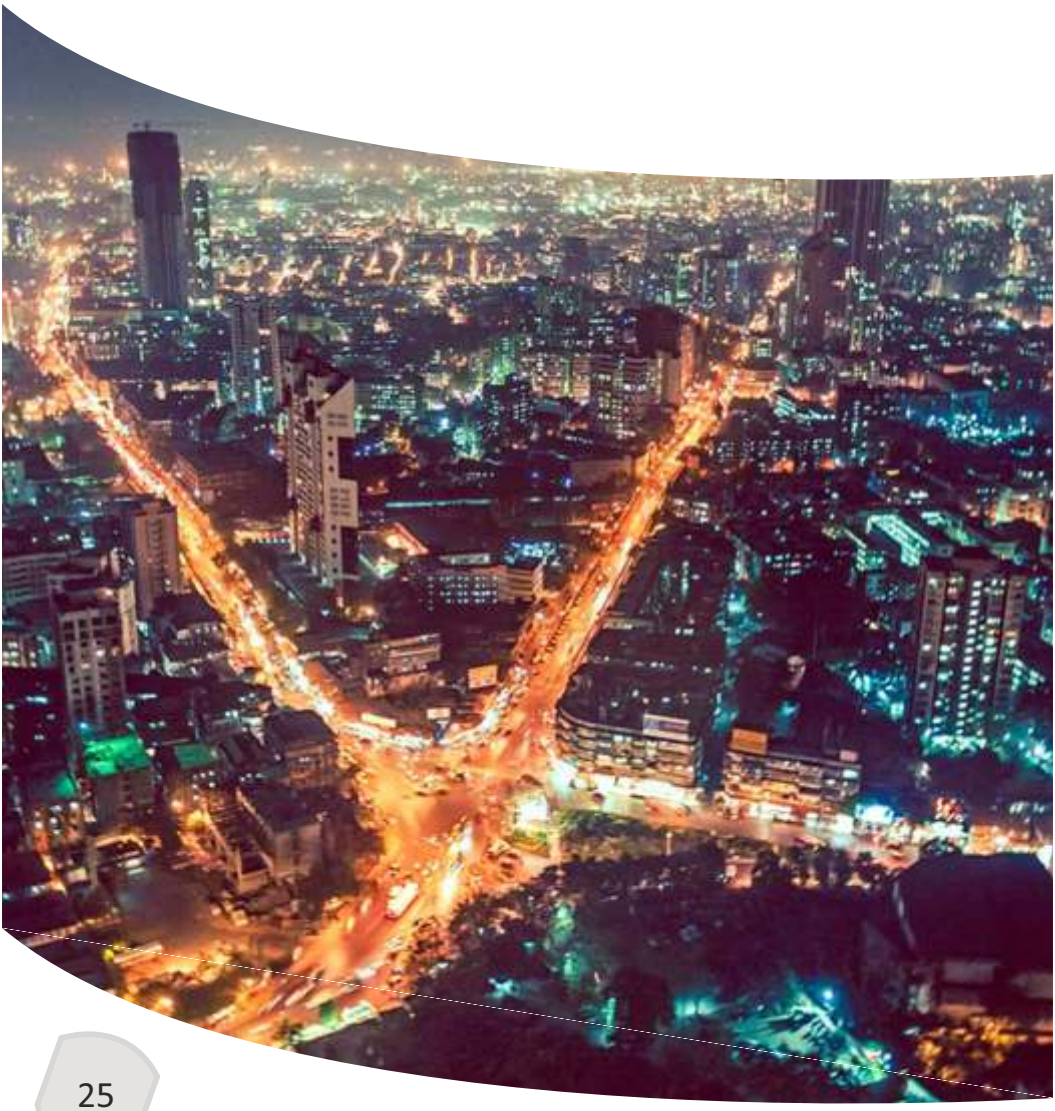
Indian Scenario

In India, currently Swine Flu has spread its roots across nearly half the country and is gradually spreading across to other regions as well. At present, the lack of adequate medications and medical coverage in remote locations is a leading cause of the influenza to spread. An unfortunate recent statistic captured in the first month of the New Year reveals worrying signs for all organizations alike. The trend is predicted to extend through the first half of the year.



ECURITY INDIA

Infrastructural Risks



Introduction

The promise of jobs and prosperity, among other factors, pulls people to urban and developing areas. 54% of the global population already lives in cities and by 2050, 70% people are expected to migrate to urban areas. However, two of the most pressing problems facing the world today also come together in these locations: these being poverty and environmental degradation.

Threats from Urbanization

The urbanization process refers to much more than simple population growth; It involves changes in the economic, social and political structures of a region. Rapid urban growth is responsible for many environmental and social changes in the urban environment and its effects are strongly related to global change issues. The rapid growth of regions strains their capacity to provide essential services such as energy, education, health care, transportation, sanitation and physical security.

One of the major effects of rapid urban growth is “urban sprawl", which implies, scattered development that increases traffic, saps local resources and destroys open space. Consequences of these effects in India, are represented by–

- Increased traffic and limited road development
- Polluted air and lack of water
- Lack of disaster management plans and preparedness
- Non-availability of agricultural land, parks and open space
- High operational costs to cater for and maintain new water and sewer lines, new organizations and establishments
- Increased requirement of police and fire protection

Solutions

Though many of these solutions may be directed or acted upon by the government, organizations are recommended to actively or voluntarily take up responsibilities in much smaller ways even through their CSR policies in regions of own interest and operations. While the

implementation would benefit the society as a whole, the solutions would also help de-risk business and operational risks arising out of global urbanization.

- Reducing income disparities among regions and creating greater job opportunities
- Reduce air pollution by upgrading energy use and alternative transport systems
- Enacting growth boundaries, parks and open space protection
- Planning for and directing employee transportation
- Creation of private-public partnerships to provide services such as waste disposal and housing
- Revitalizing already developed areas through measures such as attracting new businesses, reducing crime and improving schools
- Plant trees and incorporate the care of city green spaces as a key element in urban planning
- Preventing new development in flood plains, coastal areas and other disaster prone areas.

Conclusion

As the world continues to urbanize, sustainable development challenges will be increasingly concentrated in cities, particularly in the lower-middle-income countries where the pace of urbanization is fastest. Integrated policies to improve the lives of both urban and rural dwellers are needed.

About Us

The business environment in India is complex and filled with competing requirements, interests and incentives that must be balanced and managed effectively to ensure the achievement of key organizational objectives. The safety, security and resilience of these organizations are threatened by an array of hazards, including acts of terrorism, malicious activity in cyberspace, pandemics, man-made accidents, transnational crime and natural disasters. At the same time, risks associated with workforce management, acquisitions, operations and project costs must also be managed.

Security India helps manage these external and internal risks that have the potential to cause loss of life and assets, injuries, negative psycho-social impact, loss of economic activity, reduction of ability to perform essential functions and help enhance the confidence of workforce in the management capabilities.

Services Offered by Security India include

- Geo – Political Risk Management and Intelligence Advisory
- Security Risk Management
- Supply Chain Management and Loss Prevention
- Executive Protection and Travel Security Solutions
- Fraud Risk Management and Due Diligence
- Safety & Security Training
- Information Security & Business Continuity Management.

Leadership team

Maj (Retd) Saurabh Srivastava is a second generation Entrepreneur, an ex-army officer from the Corps of Electronics and Mechanical Engineers of the Indian Army and a seasoned Risk Consultant. An engineer at heart and an excellent analyst with deep problem solving skills, he is at the center of Security India and has remained at the forefront of assisting organizations across various segments and geographies with simplistic, holistic and cost efficient solutions to identify and mitigate a myriad of security and IT related risks.

His competency lies in securing, designing and managing of large team based complex projects. His use of ingenuity combined with expertise helps suggest and recommend implementable solutions to match clients need. He believes in the fact that every risk requires a unique solution and works diligently in providing a customised solution to mitigate the risk.

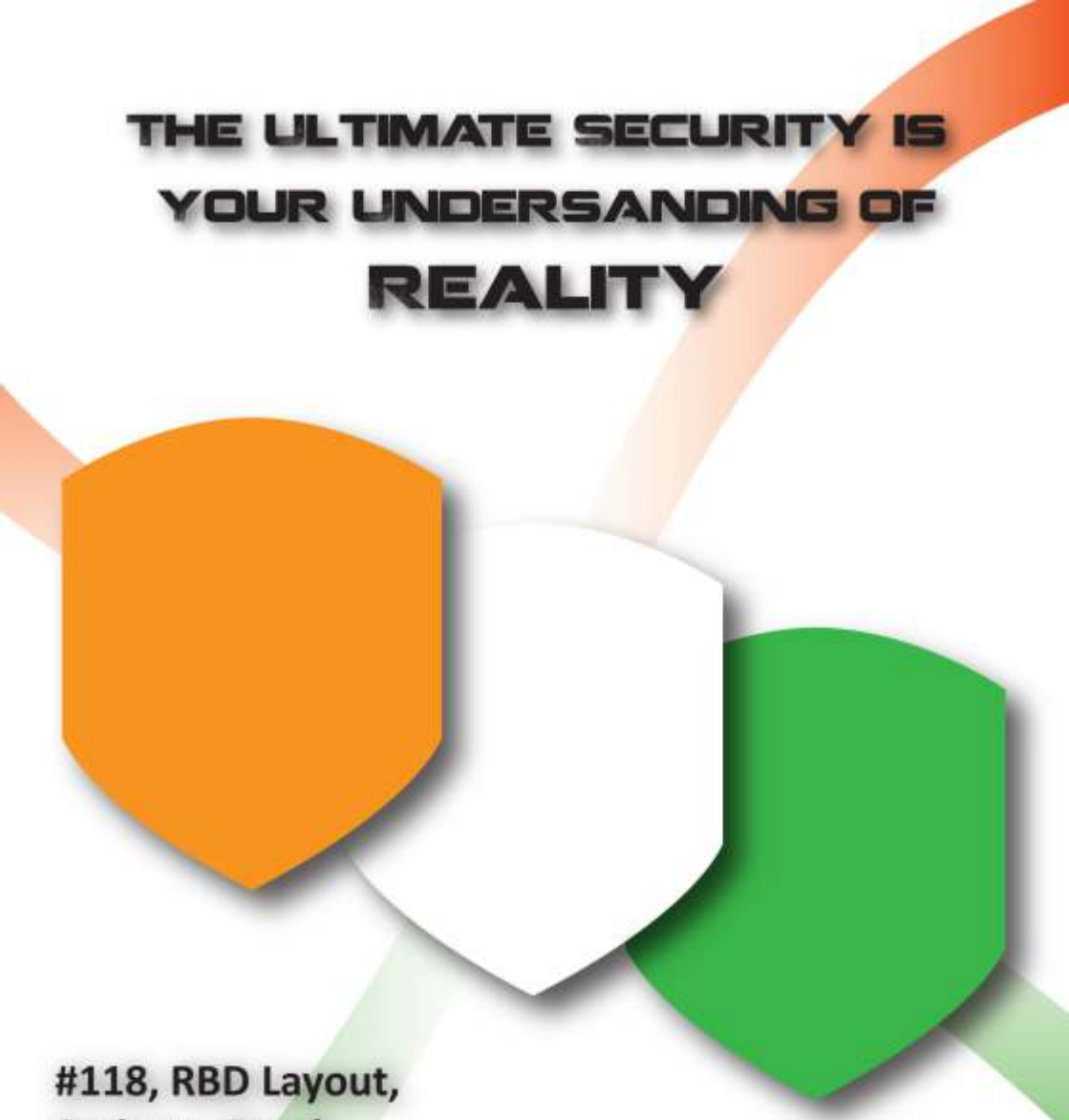
Jyoti Sahai is an engineering graduate from IIT Kanpur, and has nearly four decades of experience in banking and IT industries. His fascination and great passion for numbers and data culminated in him founding Kavaii Business Analytics India through which he offers business analytics solutions that provide actionable insights by way of KPIs and dashboards to key decision makers across diverse verticals.

His competency lies in Banking and Finance with extensive expertise in business analytics, developing performance dashboards, project management for delivery of software projects, process improvement and ERM.

Col (Retd) Dhara Chinnappa is a professional security and crisis leader with an impeccable record in the Indian Army spanning across 26 years in the most demanding conditions and inhospitable terrains. He has proved himself in various levels of leadership and has a deep understanding of people and their psychology. The expertise he gained in the army was put to good use at a multinational organization having its India headquarters in Bengaluru, for over 12 years, where he ensured creation and compliance of a multi-level security protection framework for business, people assets, facility and an exhaustive supply chain channel.

His competency lies in crisis management and problem solving where he relies on using a methodological, process driven and systematic approach to design and deliver tailored solutions to meet specific client needs.

THE ULTIMATE SECURITY IS YOUR UNDERSANDING OF REALITY



#118, RBD Layout,
Sarjapur Road,
Near Wipro Corp Office,
Bangalore – 560035
E-mail - info@security-india.com
M # - +91 9742851208

Bangalore | Pune | Hyderabad | Delhi