PINKERTON®

FICCI

INDIA RISK SURVEY

REPORT

2022



10th EDITION

Report Compiled and Written By:

PINKERTON

Ms. Mandeep Kaur
Maj. Rahul Sukhija (Retd.)

FICCI

Mr. Sumeet Gupta
Mr. Gaurav Gaur

Acknowledgements:

We would like to express our highest appreciation and deepest gratitude to all those who gave us the support to complete this report.

Disclaimer:

© Pinkerton Consulting & Investigations, Inc. d.b.a. Pinkerton Corporate Risk Management and Federation of Indian Chambers of Commerce and Industry (FICCI) 2022. All rights reserved. The content provided in the report is primarily based on data collected from the survey conducted by FICCI and Pinkerton. Though utmost care has been taken to present accurate information, FICCI and Pinkerton makes no representation towards the completeness or correctness of the information contained herein. This document is for information purposes only. This publication is not intended to be a substitute for professional, legal, or technical advice. FICCI and Pinkerton do not accept any liability whatsoever, for any direct or consequential loss arising from any use of this document or its contents.

FOREWORD



The India Risk Survey has successfully reached its 10th-year milestone, and I feel very proud to say that this survey report has helped many organizations (both private and public sector) in identifying, safeguarding themselves from the potential or prevailing risks in this dynamic business environment and also helps them to create a strategy for their risk governance.

Over the years as we introduced the Pinkerton Risk Wheel which has now matured to a more comprehensive risk governance. Risk governance involves how effectively organizations are managing risks by establishing policies, procedures, and frameworks so that the business operates in a responsible and sustainable manner. Effective risk governance is when it is implemented at the planning and strategic level of the decision-making process in an organization. To make it more effective, one should engage with subject matter experts or consulting firms who have expertise in the risk advisory domain.

This year's risk survey has outlined the top 3 risks which are Intellectual Property Theft, Information & Cyber Insecurity, and Accidents ranked in that order.

The industry leaders ranked Intellectual Property (IP) Theft as the risk which is the most prevalent threat to their business. Until 2019, IP Theft was not a part of the top 5 risks, but from 2021 it started to emerge among the top 3 risks and finally making to the number one risk this year. When we delved deeper, we could understand that the Indian businesses are understanding the processes, innovations and techniques too are valuable to a business and thus needs to be adequately protected. In the initial years of the report, most businesses only identified counterfeiting of products or violation of trademarks as an IP risk. The manufacturing of a product or the process of a service both are like soft power and need protection as much as the counterfeit product/service that may have been introduced in the market.

Pinkerton globally have been focusing on this risk and have been helping organizations make strategies to protect these Intellectual Properties via with the help of Pinkerton's Global Investigation Services with a dedicated service line of Intellectual Property Protection Service.

India Risk Survey 2022 also highlights the top 5 emerging risks which have been prevailing in this past year of 2022 and posed a threat to businesses. The most prevalent emerging risk was the "Safety and Security of Key Personnel". This risk has emerged at the top because of the threats present for the C-Suites and Directors both internally as well as externally of their business premises. The need for a safe work environment along with the safety & security required during the executive's business travels has increased manifolds in recent times and therefore, organizations are opting for Executive Protection Services to protect their key personnel from these threats.

If an organization keeps risk governance at the center when planning their risk strategies and looks beyond the realm of just compliance, it will help the organization to have an effective, comprehensive risk mitigation covering all four quadrants of risk. We hope that the report will add value to your organization's risk governance strategy.



Rohit Karnatak
Vice President – India
APAC & EMEA – Global Screening, Pinkerton

FOREWORD



Businesses are heading towards a very uncertain era and therefore, knowing our risks in advance could help us better planning their management. With an objective to sensitise businesses about the changing risk landscape in India, FICCI in partnership with Pinkerton instituted an annual exercise of gathering industry perception about different kinds of risks and publish the consolidated opinion in the form of risk ranking in an analytical report.

We entered 2022 wishing not to repeat the horrible experience of the first quarter of 2021 which witnessed the deadliest form of COVID 19 outbreak claiming lives of people around us every single day. As the businesses around the world started gaining in their volumes and activities, another disruption hit us in the form of Russia – Ukraine war, ushering in a different scenario of food and energy crises, financial uncertainties, increased cost of living and global MNCs shedding jobs and budgets.

On the policy front, a lot of brave decisions were taken by the Government to improve the internal issues and also to present India in the avatar of the Vishva Guru (World Leader). These measures have played a key role in developing resilience in the economy.

Vision of Atmanirbhar Bharat (self-reliant India) started translating into sectoral polices, regulations and creation of products & solutions, be it defence, green energy, health or digital currency. Enormous efforts have been made to relax the procedural and compliance burden on industry which resulted in improved ranking of the country under the Ease of Doing Business index. The World Bank also acknowledged that the Indian economy has been remarkably resilient to the deteriorating external environment, and strong macroeconomic fundamentals have placed it in good stead compared to other emerging market economies.[1]

Scientific know-how (like pharmaceutical, space, marine and environmental science) and application of cutting-edge technologies like cyber, AI/ML, drones, geospatial, robotics, are seen in the forefront of most of the transformational mission mode projects. Industry and especially startups are encouraged to partner with government and academia to develop India, not only as a manufacturing and export hub but also as a centre for generating knowledge and creating intellectual property.

India Risk Survey 2019 had set an alarm by ranking Natural Hazard as the second topmost risk for businesses which became number one risk in 2021. However, with the risk emerging due to climate change, compliance related to use of energy, water, emissions, disposal of hazardous substance and synthetic compounds are getting more alarming. Likewise at midst the technology threats posed by cyber criminals and rogue drones, policies to regulate intervention by stakeholders in technology space are also taking shape gradually while making them more participatory for private sector.

In nutshell, risk landscape is cyclic and the major parameters will keep on shifting depending upon the external factors, the need is to see the spectrum as a whole and plan your strategy accordingly. I hope, you will find India Risk Survey 2022 report useful to understand the risk profile of your organisation and create an appropriate risk mitigation strategy.



Manjari Jaruhar
Advisor – FICCI Committee on Private Security Industry

[1] https://www.worldbank.org/en/news/press-release/2022/12/05/india-better-positioned-to-navigate-global-headwinds-than-other-major-emerging-economies-new-world-bank-report

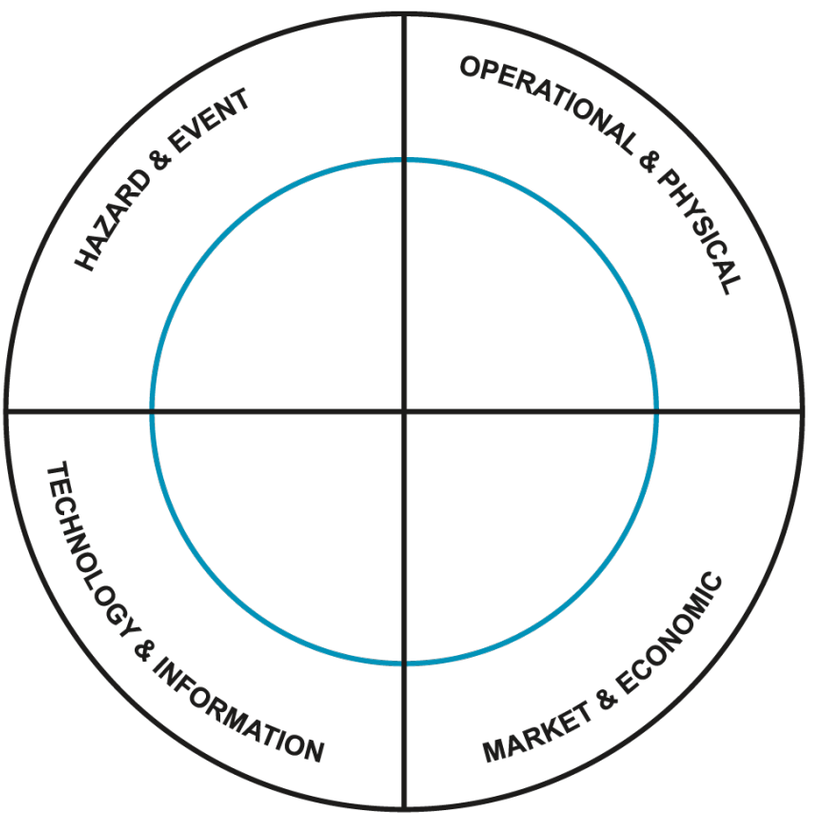
CONTENTS

EXECUTIVE SUMMARY	8
INTRODUCTION	11
RISK TREND 2022	14
TREND OVER THE PAST TEN YEARS	17
OVERALL RISK RANKING	19
REGION-WISE RISK RANKING	23
INDUSTRY-WISE RISK RANKING	27
RISK CATEGORIZATION	36
RISK IN DETAIL	37
EMERGING RISKS	65
METHODOLOGY & RESPONDENT'S	67
GEOGRAPHICAL CONTRIBUTION	68
WAY FORWARD	69
ABOUT PINKERTON	70
ABOUT FICCI	71

EXECUTIVE SUMMARY

Each year, the India Risk Survey (IRS) gathers 12 risks that, in the opinion of business enterprises and subject-matter experts, represent the most significant threats that might disrupt Indian business operations. To comprehend and evaluate each risk independently and to conduct analysis, the survey employs the Pinkerton Risk Wheel structure. The Pinkerton Risk Wheel has four different risk categories. Based on the type of threats, the risks are classified. Each quadrant has some of the risks listed under each category that are interrelated. The four quadrants in the risk wheels are Hazard & Event Risk (natural hazards, crime, terrorism & insurgency, and fire), Operational & Physical Risk (strikes, closures & unrest, threats to women's safety, and accidents), Market & Economic Risks (corruption, bribery & corporate fraud, and political & governance instability), and Technology & Information Risk (business espionage, information & cyber insecurity, and intellectual property theft).

An effective risk management strategy will address the most significant risks across all categories. By taking a 360-degree approach to risk management, organizations can effectively protect themselves from the potentially devastating effects of risk. For 360-degree mitigation and management, the India Risk Survey 2022 determines the most prevalent threat categories for each risk. The risks emphasized in this study are interrelated and cross over into other industries, sectors, and topographies.



Intellectual property theft, known as IP theft, is the unauthorized borrowing or reuse of original concepts, inventions, or other material by third parties. Companies increasingly derive value from their processes, ideas, and innovations as the world transitions to a knowledge-based economy. For companies of all sizes, intellectual property theft is a censorious issue. As a result, companies may lose millions of dollars in income, and their reputations may also suffer. Hacking into business computers, stealing original papers, and even eavesdropping on meetings are some of the ways that thieves might use to gain access to intellectual property. Intellectual property-related risks, including counterfeit goods, brand reputation loss, patent & trademark infringement, IP legal framework, and other similar issues, can lead to the loss of revenue, harm a company's reputation, and result in legal liabilities.

Information and cyber theft refer to the illegal stealing of private information belonging to another person or organization without that person's consent. The risk of cybersecurity breaches is real and growing in the current business landscape. Cybercriminals target businesses of all sizes, and the stakes are high – a successful attack can result in the loss of sensitive data, financial loss, and damage to reputation. Moreover, it can be done by innumerable illicit practices like phishing, using malware to corrupt the system or the network, and SQL injections to debauch the database, which can severely affect the integrity and security of the company. Cybersecurity threats, like data theft/phishing/hacktivism, compliance/regulatory incidents, domain-based attacks, executive threats/ impersonations/social media perils, and other cyber-related risks which can harm a company's reputation leads to the loss of confidential data, and result in legal liabilities.

Accidents at work may significantly affect any company, as they can reduce productivity, decrease sales, lower employee morale, damage reputation, and, in the worst-case scenario, force closure. Industrial accidents can have a devastating effect on businesses. The loss of life, injuries, damage to equipment and buildings, and shutdown of operations can lead to substantial financial losses. In addition, the negative publicity surrounding an accident, whether it is a road accident or an industrial accident, can damage a company's reputation eventually leading to loss of customers and business. Traffic accidents, forces of nature such as lightning, heat stroke, and landslides, factory/machine accidents, crowd mismanagement, and other related incidents can lead to business interruption, supply chain disruptions, and regulatory fines.

Business espionage often referred to as corporate spying, economic espionage, or industrial espionage refers to stealing a company's essential data and information. One of the most obvious ways business espionage can affect a company is by stealing its trade secrets. This can give the competitor an unfair advantage and lead to lost business and revenue for the victim company. The paranoia and mistrust that business espionage fosters among employees is another way that it can harm a firm. Risks, like vendor bribing, employee poaching, and other unethical practices, can result in reputational damage, the loss of business opportunities, and legal liabilities.

Despite strict legislation such as the POSH Act of 2013, Women might physiologically suffer from occupational health threats and sexual harassment, which can cause serious mental health problems. Fear of victimization causes women to alter their activities. It impacts the economy as a whole and enterprises in India. Sexual harassment-related issues, like eve-teasing, abduction, sexual favors at the workplace, sexual assault, and other similar risks, can lead to legal liabilities, reputational damage, and loss of employees.

A natural hazard is a threat of a naturally occurring event that may harm people or the environment. There are several risks connected to natural disasters which can also have grievous effects on enterprises. For instance, extreme weather can impede supply chains and transportation networks while also causing infrastructure and property damage. Wildfires and flooding both have the potential to destroy property, interrupt business, and force evacuations. Natural disasters can cause disruptions in supply chain management and equipment loss, leading to revenue loss just like the COVID 19 pandemic did.

When it comes to fire safety, there are a lot of possible concerns that organizations might encounter. Using combustible materials, electrical equipment, and culinary appliances can provide operational hazards that increase the possibility of a fire breaking out on a corporate property. Also, ineffective fire safety management may raise the probability of a fire. When a fire breaks out at a place of business, the results can be disastrous as it may affect the viability of the enterprise along with the physical damage that occurs on the business premise. A fire can also have a significant negative impact on the company, disrupting operations and resulting in financial loss. Fires caused by electric short circuits, chemical-based incidents, and gas cylinder/stove bursts, can cause harm to people and property, interrupt business operations, and cause revenue losses.

No company is safe from crime. Businesses may unintentionally participate in a crime or become its victims. In addition, crime may significantly affect a business regarding direct and indirect expenses. For example, in regions where drug trafficking or arms trafficking is prevalent, businesses may face higher levels of violence, theft, and

corruption. This can make it challenging to operate effectively and creates an unstable business environment. Similarly, kidnapping, extortion, and burglaries can lead to financial losses and impact the safety of employees and customers. The price of stolen products, the price of repairs following a break-in, and the price of more stringent security measures are some examples of the direct costs of crime. The indirect costs, sometimes more challenging to calculate, might include lost clients, lost employees, and reputational harm to the company.

Inefficiency and other administrative failings have plagued and continue to confront varying degrees of cultures worldwide. Political instability can have a multitudinous influence over many areas of business risk, specifically the effects of a country's financial and economic situation. The Indian political landscape has been volatile in recent years. This has made it difficult for businesses to plan for the future. Centre-state conflicts can create a significant level of uncertainty in a country, which can negatively impact businesses operating in the affected states. State fragility, policy changes, local government instability, and international conflicts can lead to supply chain disruptions. These conflicts can take various forms, such as disagreements over resource sharing, jurisdictional boundaries, political control, and ideological differences. However, India's standing in the world's Ease of Doing Business rankings has significantly improved in recent years. Several business-friendly initiatives and policy decisions made by the federal, state, and local governments are important contributors for the aforementioned.

Corruption may have a high financial cost. Bribery and corruption may force corporations to pay more for goods and services. This may result in lower profit margins and harsher competition. Inefficiencies can also be brought on by corruption. Unethical business practices, like bribery/kickbacks, shell companies, conflict of interest, business identity theft, and other such issues, can lead to legal liabilities, reputational damage, and a loss of business opportunities. For instance, a business would need to submit extra paperwork or go through additional approval procedures to complete tasks. Time and money may be lost in this. Reputational harm is another price of corruption. A company's reputation may suffer, and it may be more challenging to secure new business if it is discovered to have bribed authorities or engaged in other corrupt activities.

Any organized absence from work by a group of workers or employees in favor of a demand they have made is referred to as a strike. These include work slowdowns, go-slows, overtime restrictions, and work-to-rule. Strikes can have a significant impact on businesses, both in the short and long run. In the short run, businesses may have to deal with lost production, increased costs, and disruptions in their operations. Union/labor strikes, civil unrest, political violence, regulatory changes, and other labor-related issues, can interrupt business operations, result in the loss of revenue, and may harm the company's reputation. In the long run, strikes can damage relationships with customers and suppliers and lead to a loss of business.

Terrorism is the deliberate, coordinated, and routine use of force to achieve political, religious, or ideological ends. Terrorist threats, includes active shooter/suicide bombers/insider threats, explosives, CBRNE, narco-terrorism, and other similar risks that can result in the loss of life, damage to property, and restrict a range of economic activities. It has spread globally and severely threatens world peace, security, and stability. In addition, business groups spend more on security due to insurgency. This results in paying for private security services and safeguards.

INTRODUCTION

FICCI and Pinkerton publish the India Risk Survey (IRS) report to identify possible business risks and difficulties prevailing in the Indian business landscape. The survey identifies 12 key areas of concern for businesses and 5 emerging risks that might seriously damage India's business ecosystem. The results are derived from a survey that involved stakeholders and business executives from various industries.

The India Risk Survey Report is frequently seen as a significant predictor of the risks that Indian firms must deal with. Businesses use the report to evaluate their risk exposure and decide how to operate in India. In addition, the media and decision-makers frequently use the survey's conclusions as proof of the difficulties experienced by Indian entrepreneurs.

The India Risk Survey Report gives valuable information about the risks that firms face, like Natural Hazards, Information & Cyber Insecurity, Intellectual Property Theft, Fire, and Crimes, and enables them to make defensible choices regarding their operations.

Surpassing the risk of Natural Hazards and pandemics, the risk focus has drastically shifted to Intellectual Property Theft and Information & Cyber Insecurity due to the increasing interconnectivity of businesses' reliance on technology, and the vast amounts of data that are now stored electronically. Offices have been replaced by hybrid working arrangements, and growing digitization has accelerated the threat.

Cases of industrial accidents along with road accidents have been rising as they occur suddenly and without warning, often causing extensive damage to property and equipment. They can also lead to injuries or even fatalities, leading to both reputational and revenue damage for the business.

While business espionage is not a new phenomenon, but it has become more prevalent in recent years as the world of business has become more globalized. Companies are now operating on a much larger playing field and there is more at stake.

The goal of this survey is to identify potential risks in the context of a changing global environment, allowing business leaders to assess their circumspection for disruptive events like rapid digitalization, accidents, and business espionage, in the future and to ameliorate risk mitigation techniques. Nonetheless, based on each industry's risk appetite and current risk mitigation plans, the risks identified and their effects may differ from one to the next.

The survey's outcome will help organizations create a 360-degree risk management strategy that will allow them to foresee and prepare for any eventuality, limit interruption, and protect against any risks in advance.

Risk is everywhere but its manifestations are changing. We as people have barely recovered from one of the deadliest pandemics in history, only to be thrust into a series of geopolitical risks in the form of the Russia-Ukraine conflict, China-Taiwan tensions, and US-Russia tensions. We have recently been celebrating over a hundred unicorn startups created in India, only to see the Silicon Valley Bank collapse creating a cascade of caution from VCs, tightening crucial liquidity to startups. We have witnessed the devastation caused by deadly earthquakes in Turkey and Syria and are at the same time hearing of dire forecasts of heatwaves for the Indian subcontinent. We have experienced the euphoria of a truly intelligent 'chatGPT' only to be unsettled by its near-sentient conversations and eerie musings. There are a few underlying patterns in the manner these risks are occurring now and in the way they are being addressed.

India as a geography also faces unique risks and opportunities, some of which may differ from other countries. The IRS survey captures the risk patterns well and clearly highlights that some of the most existential risks for us today in India are based on cyber-security and IP protection and climate change. Most of these risks would have barely been blips on an executive's radar fifteen years back. Multiple industries are showing shifts in risk patterns. Let's take Defence as an example. As we speak, we are already seeing the future of warfare and defence unfold before our eyes. Recently the US shot down a spy balloon, waking us up to an era of warfare from the outer edges of space. The Russia-Ukraine conflict has shown us glimpses of the unmanned nature of warfare, even as the conflict enters the second year. Drones have taken centre-stage in the ongoing narrative and the ways our skies are patrolled and protected are changing forever.

The new era of warfare opens us up to unusual and new risks, where attacks can be coordinated from thousands of miles away, at the click of a mouse. Securing our future therefore means being proactive & vigilant, being organized & being connected. In many ways, these changing risks reflect shifts for the new India – one of the most populous countries on earth, hyperconnected, fast-growing, data-savvy, and service-led, yet vulnerable to basic food / energy / security challenges. Global risk trends have a cascading effect on India as well. The tensions between US and China are resulting in shifts of manufacturing bases towards India for higher end products like smartphones, electronics, automobiles, among others. Global supply chains are increasingly getting fractured and localized in the wake of geopolitical tensions. Defence spending is increasing rapidly as countries hustle to scale up their capabilities and secure their borders. We are thus moving from a globalized world to a multi-polar and fragmented world. India is likely to be a lynch pin in the emerging world order. Thus, we are at a crossroads in time as a nation - a time of crisis and a time of opportunity, a time of caution and a time of resilience, a time of Atmaraksha and a time of Atmanirbharta.

We must prepare to lead the new world order while managing the risks that come with the transition. We need to ensure our IP is protected, even as we claim our rightful place in the global stage as a business powerhouse. We have to ensure that our assets are cyber-secure even as our networks expand. It is an onerous task. Technology will be a key enabler for us to navigate the complex world ahead. The products we make and services we offer need to have security and IP protection aspects baked into the core design itself. Climate friendly technologies need to help manage our transition to a cleaner & more sustained future. While India, as the world's fastest growing major economy provides a rich canvas for local players, we as industry leaders can take India into 'game-changing' territory only if we go global with some of these offerings.

Additionally, the business environment in which we conduct our dealings

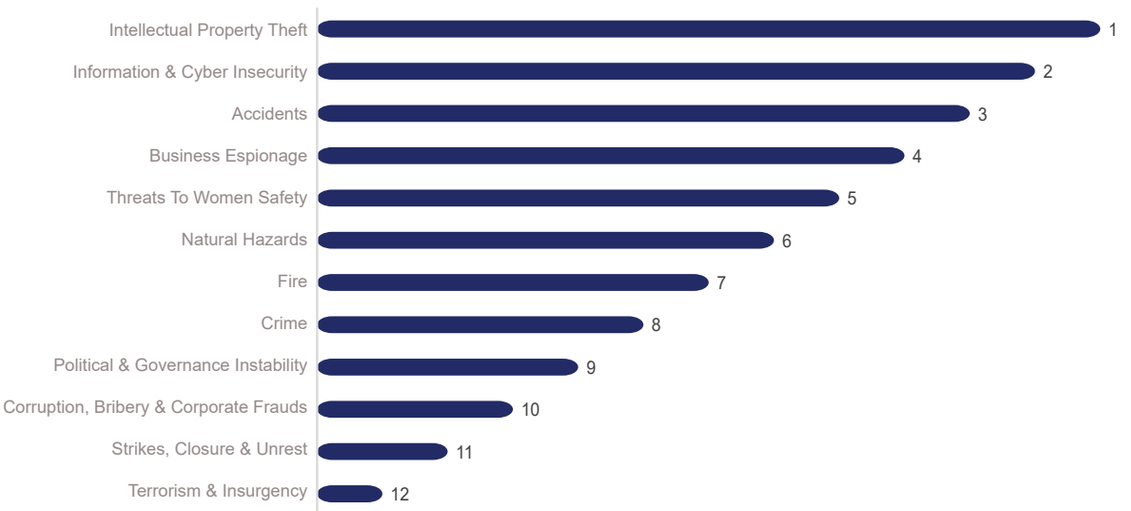
needs to reflect emerging threats and risks as well. Fracturing supply chains bring with them a whole host of local nuances to be addressed – approvals, new business setups, testing and quality certifications and new supply chain integrations, to name a few. Each of these requires a friendly policy environment as well as decisive organizational shifts. Climate change will bring out hitherto unseen disruptions to human health, safety and security – companies need to adapt to these new working conditions effectively, especially in domains where exposure to heat/weather conditions is high. Lastly, we need to talk about capabilities.

Risk is no more just the domain of the CEO or the Chief Risk Officer (CRO). Each function and stakeholder need to consider themselves a Chief Risk Officer of their domains and ensure that risks are adequately called out, mitigated judiciously and the lessons captured diligently. Organizational structures need to develop horizontal capabilities that help capture these micro and macro risks and help mitigate them before they threaten the underlying fundamentals of business.

To conclude, while risk is ever present and shifting, it is also clear that opportunity lies within. Winning players need to tread the fine line between opportunity and risk & pull together an ecosystem wide approach to managing and mitigating risk – leveraging technology, building risk capabilities deep into their organizations and carefully navigating the business environment in which they operate. Most importantly, India is in pole position to demonstrate how it can navigate an uncertain global environment and claim its rightful place in the world order. As citizens and as stakeholders, it is our duty and opportunity to help India in this journey.”

Mr Ashish Rajvanshi
Chair, FICCI Committee on Drones and
President & Head, Chairman's Office, Adani Group

RISK TREND 2022



Intellectual property theft, information & cyber security threats, and accidents were ranked as the top three business threats in India by survey respondents for this year's India Risk Survey. In contrast, "Threats to Women Safety" rose from 12th place in 2021 to 5th place in 2022. With increasing reports of violence against women, it has become clear that companies must take measures to ensure the safety of their women employees and customers. According to survey participants in India, this year, the lowest risk is associated with terrorism & insurgency.

Intellectual Property Theft has swarmed up to the top spot. Since, business intellectual property can be swiftly monetized, therefore, cybercriminals and dishonest personnel frequently target it. These personnels and cybercriminals seize several chances in this digital age to secretively duplicate trade secrets, copyrights, patents, and trademarks and sell them to rivals. By proactively identifying these risks, corporates can think about adding a new business-focused strategy to contracts and legal remedies for revamped IP Management.

Information & Cyber Insecurity has retained its second position because businesses are becoming more exposed to cyber thieves as they have started to store more of their data online. Rapid digitalization along with hybrid working models have led to data thefts, ransomware, disrupted business, and tarnished brand equity which has increased the financial burden for the industries. Assessing the viability of different security risks in businesses and determining the effects of cyberattacks are the major goals of risk identification. Based on this information, an effective security system can subsequently be built to protect the IT systems from "Hacktivists".

Accidents have been ranked at third position as frequency of accidents have increased in the recent times resulting in severe physical and/or mental harm to employees. Accidents also impacts the business financially as additional cost is borne by the firms in terms of victim compensation and financial loss due to production halt. It also negatively impacts the company's reputation in the market. Businesses should put a great deal of effort into preventing workplace accidents at all costs by using state-of-art technology and creating a secure workplace for their valued employees.

Business Espionage which is ranked at the fourth position entails the use of listening or monitoring devices, covert cameras, and transmitters, as well as cyberattacks in which systems are compromised and sensitive data is accessed, copied, or stolen. Business espionage is occasionally carried out by spies who infiltrate companies to

gain confidential information by stealing or copying data or searching through paper trash, among other methods. These spies may be current or past workers, housekeepers, contractors, or trespassers. Businesses should take holistic measures to safeguard their trade secrets and be vigilant and keep an eye out for their competitors' activities.

Women experience discrimination and harassment from their co-workers at work regularly which has become more evident as **Threats to Women Safety** has been ranked at fifth position this year. The workplace has evolved into a considerably more diversified environment during the last three decades. Personal security and safety has become essential to women's physical, intellectual, emotional, economic, and spiritual well-being in India, where women constitute 22.2% of the workforce.[2] Quid pro quo and hostile working environment is causing a lot of women to go through psychological and physiological trauma, which compels them to leave their jobs. This causes a lot of revenue and reputational damage to the firms. Companies should adopt efficacious sexual harassment policies, create awareness, and set up an Internal Complaints Committee (ICC) for woman grievant where they can freely express themselves.

Top Three Risks in Each Region of India

	RISK RANK 1	RISK RANK 2	RISK RANK 3
NORTH	Information & Cyber Insecurity	Intellectual Property Theft	Natural Hazards
SOUTH	Accidents	Intellectual Property Theft	Information & Cyber Insecurity
EAST	Intellectual Property Theft	Accidents	Fire
WEST	Intellectual Property Theft	Information & Cyber Insecurity.	Accidents

The above table presents the top three risks faced by various regions in India, ranked in order of severity. The North region is most vulnerable to information & cyber insecurity, with intellectual property theft and natural hazards coming next. In the South, the most significant risk is accidents, followed by intellectual property theft and information & cyber insecurity. The East region is at high risk of intellectual property theft, with accidents and fire being ranked at second and third position. Finally, in the West, the most prominent risk is intellectual property theft with information & cyber insecurity and accidents follow closely on their heels. Understanding these regional risk rankings can help individuals and organizations take appropriate measures to protect themselves and their assets from potential threats.

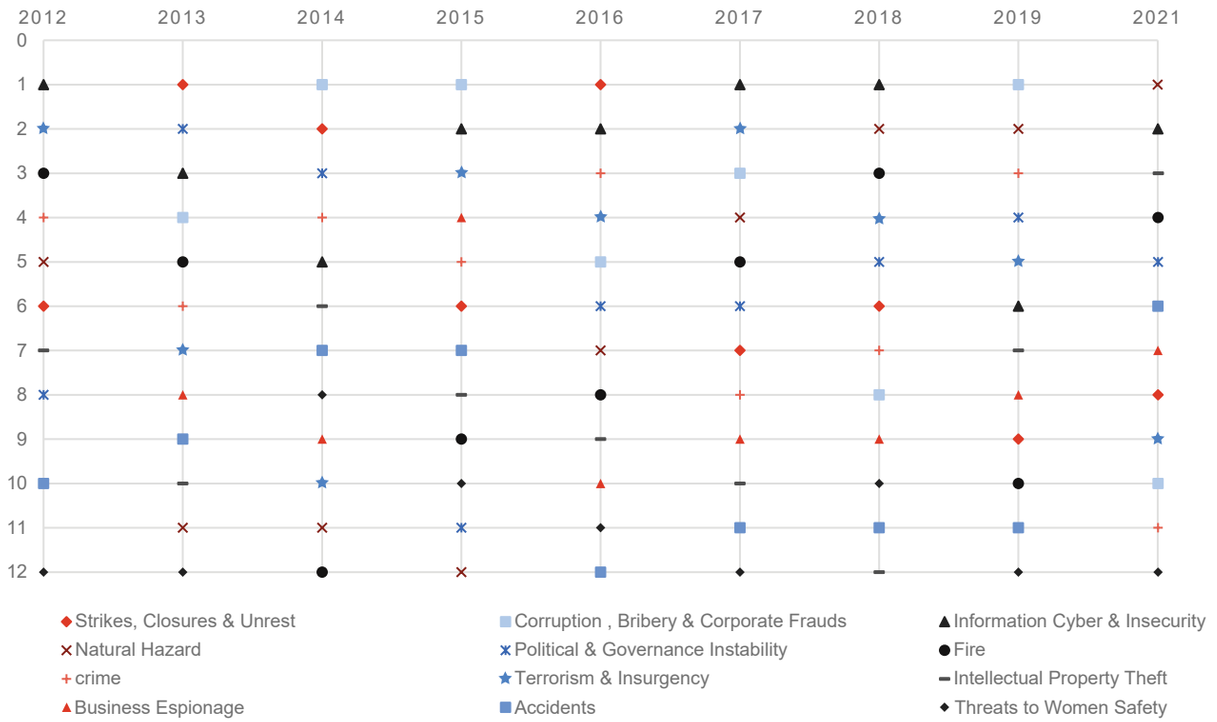
[2] https://www.india-briefing.com/news/women-and-work-in-india-trends-and-analysis-24758.html/

Top Three Risks Across Industry Sectors

The majority of respondents chose “Intellectual Property Theft” and “Information & Cyber Insecurity,” as their top risks when it comes to industry-specific risk segmentation, followed by “Business Espionage,” “Accidents,” “Natural Hazards” and “Fire” among the key risk parameters.

	RISK RANK 1	RISK RANK 2	RISK RANK 3
IT / ITES	Information & Cyber Insecurity	Intellectual Property Theft	Business Espionage
MANUFACTURING	Accidents	Intellectual Property Theft	Business Espionage
CONSULTING	Information & Cyber Insecurity	Business Espionage	Intellectual Property Theft
REAL ESTATES	Intellectual Property Theft	Accidents	Natural Hazards
EDUCATION	Intellectual Property Theft	Business Espionage	Information & Cyber Insecurity
SECURITY SERVICES & SOLUTIONS	Intellectual Property Theft	Business Espionage	Information & Cyber Insecurity
FINANCIAL SERVICES	Information & Cyber Insecurity	Intellectual Property Theft	Business Espionage
HOSPITALITY	Natural Hazards	Intellectual Property Theft	Accidents
LOGISTICS	Intellectual Property Theft	Accidents	Fire
CONSTRUCTION	Accidents	Intellectual Property Theft	Crime
RETAILS	Accidents	Intellectual Property Theft	Natural Hazards
MEDIA AND ENTERTAINMENT	Information & Cyber Insecurity	Business Espionage	Fire

Trend Over The Past Ten Years



The Indian business ecosystem has faced several risks over the past 10 years. These risks can be broadly classified into intellectual property theft, natural hazards, political & governance instability, accidents, terrorism & insurgency, fire, information & cyber insecurity, crime, strikes, closure & unrest, corruption, bribery & corporate frauds, business espionage, and threats to women's safety. These risks have constantly been damaging the business ecosystem of India.

Natural hazards have been among the biggest risks to the Indian business ecosystem over the past 10 years. In 2012, natural hazards were placed at the fifth position and then kept declining until 2015 at the last spot. Later, the natural hazards risk kept climbing up the ladder and reached the second position in 2018 and 2019. The biggest naturally occurring risk was the Covid 19 Pandemic which devastated the entire business process across the globe and increased the financial burden on the economy. Following this, respondents ranked the natural hazards at the top position in 2021 as it caused severe supply chain disruptions and inflation in the market.

Political & governance instability has also been a major risk for the Indian business ecosystem. Economic growth is often catalysed by clear and long-term vision of governments with effective enforcement of laws, regulations and synergies among federal and state governments. Lack of strong political will and frequent changes in government structure, mindsets and policies create uncertainties for businesses. Political & governance instability was ranked at second and third position in 2013 & 2014, it disappeared from the top five risks years during 2015-17 with the change of government, and again spotted in the five most concerning business threats in 2018, 2019, and 2021.

Terrorism & insurgency pose a higher risk because there have been several terrorist attacks in India over the past 10 years. From 2015 to 2019, it was constantly fluctuating between the 3rd to 5th spots. However, strict measures being taken by the Government have minimized the risk and thus ranked at the 9th position in 2021.

There have been several major fires in India, and therefore, the risk of fire was ranked 3rd in the year 2012 and 5th in the year 2013. Later on, it dropped to the lowest rank in 2014. It steadily increased until 2018, when it again reached the 3rd spot. In 2019, it again collapsed to the 10th position. Nonetheless, it again jumped to the 4th spot in 2021.

Information & cyber insecurity has become a huge risk for businesses in India due to the growing number of cyber-attacks. This risk has always been in the top five positions except in 2019, making it the most prevalent threat across different industries. In 2012, 2017 & 2018, it was ranked at the first position due to the rapid digitalization in the country.

Intellectual property theft has been a critical concern for businesses across India. In 2012, it was rated at the 7th place and then dropped to 10th in 2013. It has consistently decreased up to the last spot till 2018. Eventually, due to the rising digital conversion, it climbed to the third position in 2021.

Crime has also been a major risk for the Indian business ecosystem. In 2012, Crime was voted at the 4th position and then dropped to the 6th position in 2013. Subsequently, it always ranked in the top 5 until 2016 and again fell to lower positions in 2017-18. In 2019, it rose to the third position.

Strikes, closure, & unrest are major risks for the Indian business ecosystem. This is because India has had several major strikes and protests over the past 10 years, including the Jat quota agitation of 2016,[3] the Bharat Bandh of 2018[4] and Kisan Andolan of 2020-21.[5] It ranked 6th in 2012 and climbed up to 1st position in 2013 and 2nd position in 2014. Again, it sank to the 6th position in 2015 and rose to Rank 1 in 2016, showing major fluctuation.

Corruption, bribery and corporate frauds have also been major risks for the Indian business ecosystem. With several high-profile corruption scandals coming to light, corruption has always ranked higher. In 2014 & 2015, it was the highest-rated risk faced by companies across India. In 2016 & 2017, it was ranked in the 5th and 3rd position, respectively. Later, in 2018, it dropped to the 8th spot and again, in 2019, it escalated to the first position. However, in 2021, it sank to the 10th spot.

Business espionage has also been a major risk for the Indian business ecosystem. In 2013 & 2014, it was positioned in 8th and 9th place, respectively. It rose to the 4th spot in the year 2015. Later on, it remained at the lower risk until 2021.

Accidents have been a cause of concern for the businesses due to the increase in the cases of road and industrial accidents every year. It was ranked at the 10th, 9th & 7th position in 2012, 2013 & 2014, respectively. In the year 2016, it fell to the lowest rank. It was constantly positioned at the 11th rank in 2017, 2018 & 2019. Then it jumped to the 6th spot in 2021.

Threats to women safety have also been a major risk for the Indian business ecosystem. It has mostly ranked at the lower spots. However, in 2022, it rose to the fifth position demonstrating the violence women face in the workplace. The rise of violence against women in the workplace has been linked to a lack of awareness about safety protocols and inadequate security measures.

A risk analysis assesses the likelihood of an unanticipated disastrous event that could impact critical business activities and projects. Companies undertake risk analyses to determine when a negative outcome is possible, how the risk may affect a particular business sector, and how the risk may be reduced. A business study creates a control plan to return corporate operations to normal in the worst-case scenario of an unanticipated unfavourable impact.

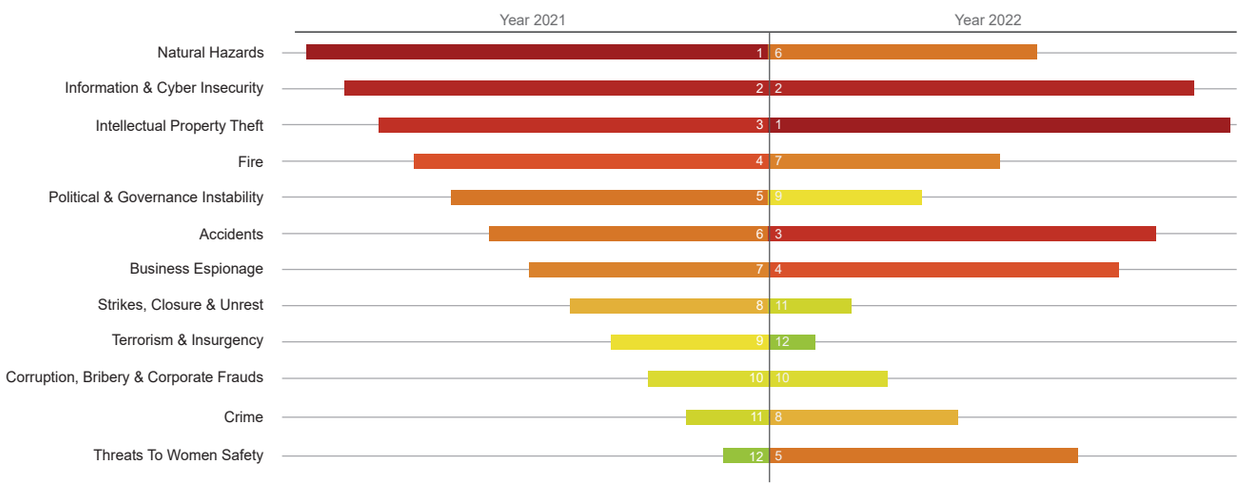
[3] https://en.m.wikipedia.org/wiki/Jat_reservation_agitation

[4] https://www.google.com/amp/s/www.jansatta.com/rajya/bharat-band-bharat-bandh-2018-today-news-10-april-2018-in-madhya-pradesh-karnataka-banglaore-latest-news-updates-protesters-have-stopped-train-in-bihar/626546/lite/

[5] https://m.economictimes.com/news/india/thousands-of-farmers-march-towards-delhi/articleshow/83299515.cms

In the above trend analysis, the risk of Natural Hazards didn't just occur in 2020. It has been prevalent since 2017 when it was ranked in the 4th position. In 2018 and 2019, it was alarming when it reached the 2nd spot. Companies that followed the trend analysis, were prepared for the remote working model beforehand and they thrived in the crucial situation when the entire global economy was at the risk.

OVERALL RISK RANKING



India Risk Survey 2022 study identifies 12 broader threats that business leaders believe could or have already disrupted operations. The most prominent threat under each risk, as ranked by respondents, has been highlighted by IRS 2022. This study aims to inform businesses, help them plan, carry out mitigation measures, and guarantee continuity.

"Intellectual Property Theft" has risen to the first position while "Information & Cyber Insecurity" stands steady at the second position due to the hybrid working paradigm and reliance on digital infrastructure. The top five threats for 2022 are "Accidents," "Business Espionage," and "Threats to Women's Safety" along with "Intellectual Property Theft" and "Information & Cyber Insecurity."

In addition to the traditional risks which always remain there in the minds of the business leaders and risk managers, some new concerns keep on appearing from time to time. Many of these emerging risks are not very impactful, but some can really disrupt businesses and leave a long-lasting impact. India Risk Survey every year check the

pulse of business houses on emerging risks. In year 2022,"Safety & Security of Key Personnel," "Compliance Related Risks", "Health Risks," "Loss of Employees (Employee Turnover)," and "Resilience Risk" have been the major emerging concerns for the business environment. Ensuring the safety and security of important individuals within the organization, such as executives or other high-profile employees is critical in order to maintain business continuity and reputation. Compliance-related risks can result in both financial and reputational damage, while health risks and employee loss can impact productivity and lower the employee morale. Finally, resilience risk, which refers to the potential impact of disruptive events, such as natural disasters, cyber-attacks, or supply chain disruptions, on an organization's ability to operate effectively, requires organizations to develop and implement comprehensive risk management plans to mitigate the potential impact of these events.

In the 2022 survey report, the trend of intellectual property theft emerged as a top risk. This is likely due to the rapid digitization and rise of competitive landscape, where individuals and companies may attempt to steal trade secrets. This is particularly concerning for companies who have invested significant resources in developing unique concepts, as cheaper copies of their ideas may emerge in the market, posing a threat to their business. This risk was positioned at the third rank during the IRS 2021 survey due to the increasing cases of IP theft in the country.

"Information & Cyber Insecurity" has retained its second spot due to the remote working model and increased dependency on technological infrastructure.

"Accidents", "Business Espionage" and "Threats to Women Safety", rounds up the top five risks of 2022. "Threats to Women Safety" has jumped from the last position in 2021 to the fifth spot in 2022 throwing light on the gender disparity across the country.
While "Corruption, Bribery and Corporate Frauds" is sitting at the 10th position as the last year, "Fire" has gone down to the 7th spot.

Due to the consistent efforts made towards curbing terrorist outfits & activities and providing mechanism in government policies to ensure equal rights to all sections, the risk of "Terrorism Insurgency" and "Strikes Closure & Unrest" has sunk to the 12th & 11th spots respectively as compared to the 9th & 8th spots, last year.

Factors Influencing the Top Risks

INTELLECTUAL PROPERTY THEFT



TRENDS: The horrifying discovery that a company's network breach has happened, and that sensitive intellectual property is now in the hands of unidentified parties is the nightmare of every businessman. IP thieves can work anonymously anywhere in this digital world, which expands the range of suspects. Respondents ranked Intellectual Property Theft as the most prevalent risk due to the growing threat that it poses to businesses from cybercriminals, IP copyright pirates, brand imposters, patent trolls, and trade secret thieves.

THREAT MAPPING: A company may be exposed to significant risks of intellectual property theft, including the technical data, business processes, data sets, and other sensitive information, due to the increased reliance on technology and a shift in the composition of many companies' assets away from traditional brick-and-mortar assets and towards intangible ones. With the rise of globalization, the awareness regarding the same is also increasing amongst the business owners. As a result, more people are reporting cases of IP infringement and theft, which can result in severe financial losses and reputational damage for companies.

Due to the Government's efforts to improve the nation's Intellectual Property Rights (IPR) framework, the number of patent submissions climbed from 42,763 in 2014–15 to 66,440 in 2021–22.

In addition, a remarkable increase has been witnessed in the numbers of patents granted in India which reached to 30,074 patents in 2021–2022 versus 5,978 in 2014–15.[6]

Copyright holders continue to claim substantial amounts of piracy, primarily on the internet and through commercial broadcasts, despite positive efforts made in online copyright enforcement. This covers persistent problems, including illicit file sharing, software, and data theft, and getting around technology protection measures. Rapid digitization has led to a surge in the piracy of digital content, with India's music piracy rate at an alarmingly high 68%, according to a report published by the Indian Music Industry (IMI) in April, 2022. The consequences of piracy are significant, leading to billions of dollars in losses for the entertainment industry and an 11% loss in employment in the Indian film industry, according to research by the US-India Business Council. Despite the efforts made by central and state enforcement agencies, the issue of intellectual property theft has been an evident concern for businesses and needs more attention from the Government. Companies must take additional steps to protect their intellectual property in India, such as partnering with local law enforcement agencies, investing in stronger security measures, and advocating for stronger intellectual property protection laws.[7]

While laws cover practically all intellectual property rights and enforcement methods, the legislative process is lengthy and tedious. The same problems may not be resolved for years. This can make industries' strategic intellectual property and enforcement decisions more difficult and ambiguous.

INFORMATION & CYBER INSECURITY



TRENDS: Respondents have ranked Information & Cyber Insecurity as the second most important concern in the 2022 study, due to digital revolution and adoption of hybrid working models.

THREAT MAPPING: With the increasing use of digital devices and systems, the concern for cyber safety and security has increased manifold in recent years. Companies and organizations have incorporated it as a part of their core planning stage and recognized the importance of protecting their digital assets and sensitive data. Cybersecurity risks such as data breaches, ransomware attacks, and phishing scams can cause financial losses, damage to reputation, and legal repercussions for businesses. As such, it is essential for companies to have robust cybersecurity measures in place like conducting regular security audits, employee training on best practices of cybersecurity, and implementing up-to-date security software and protocols.

According to CERT-In data, there were 41,378 cyberattacks in 2017 and 14,02,809 attacks in 2021. However, this number has slightly dropped in 2022, where 13,91,457 cyber security incidents were observed in 2022. Since the pandemic, organizations have implemented the necessary work-from-home infrastructure, leaving businesses, especially those in the IT/ITES sector, vulnerable to cyberattacks, fraud, and data theft. However, with the return to office phase beginning, this year's attacks have been fewer than the previous year.[8]

ACCIDENTS



TRENDS: An accident at work is the third top risk among the many concerns that plague business owners while they manage their enterprises and its operations.

[6] https://pib.gov.in/PressReleasePage.aspx?PRID=1815852

[7] https://www.hindustantimes.com/ht-insight/economy/india-needs-stronger-copyright-and-ip-laws-101660202940185.html

[8] https://www.business-standard.com/article/current-affairs/cyber-security-breaches-are-up-multiple-times-as-internet-penetration-grows-123021900451_1.html

THREAT MAPPING: In India, road accidents claimed approximately 1.55 lakh lives in 2021, or an average of 426 per day or 18 per hour. According to official government data, these are the greatest death rates reported in any calendar year to date.[9]

According to data gathered by global workers' union IndustriAll, , the industries with the greatest fatalities in India are manufacturing, chemicals, and construction. According to the report, seven accidents were reported on average per month in India's manufacturing sectors in 2021 alone, killing more than 162 people. The Delhi police in 2022 said that 663 factory accidents were reported in the city over the previous five years, resulting in 245 fatalities. A total of 84 persons were detained for these mishaps.[10]

BUSINESS ESPIONAGE



TRENDS: Business Espionage has climbed to fourth in the risk ranking. Business espionage entails watching the rival company learn about their top-secret business dealings. There are several ways to spy, including listening in on phone conversations, breaking into computer networks, or even paying off former and present employees to learn the plans of rival companies. Almost every business institution engages in this practice; the only difference is that some were discovered in time, while others continue making money from the ideas of others.

THREAT MAPPING: India is one of the top 5 countries in the APAC region targeted by cyberattacks, notably security lapses including cyber espionage.[11] Corporate espionage is increasingly becoming common and can pose significant risks to businesses. It involves the use of illegal means to obtain confidential information, such as trade secrets, financial information, and client lists. Perpetrators of these crimes can be competitors, employees, or third-party vendors. Small and medium businesses are also at risk of corporate espionage, along with the large corporations. It is important for businesses to take proactive steps to protect themselves against corporate espionage by implementing strong security measures, conducting regular risk assessments, and training employees to be aware of the risks. Cyber-attacks are also a growing concern for businesses and contributes in the theft of sensitive information or disruption of business operations.[12]

THREATS TO WOMEN SAFETY



TRENDS: Threats to Women Safety Risk has climbed to fifth in the India Risk Survey 2022. Despite several measures being taken by the Government, women's safety has been a concern, both in the workplace and outside.

THREAT MAPPING: The National Commission for Women (NCW) in India reports that in 2022, it received more than 30,000 complaints about crimes and acts of violence against women, which is a record-high number compared to 2014. The offense of molestation was the subject of more than 2500 complaints. More than 1500 complaints concerned rape and attempted rape; more than 1500 others involved police hostility against women.[13]

[9] https://auto.hindustantimes.com/auto/news/road-crashes-claimed-18-lives-every-hour-across-india-in-2021-government-data-41662290089954.html

[10] https://www.bbc.com/news/world-asia-india-62631699

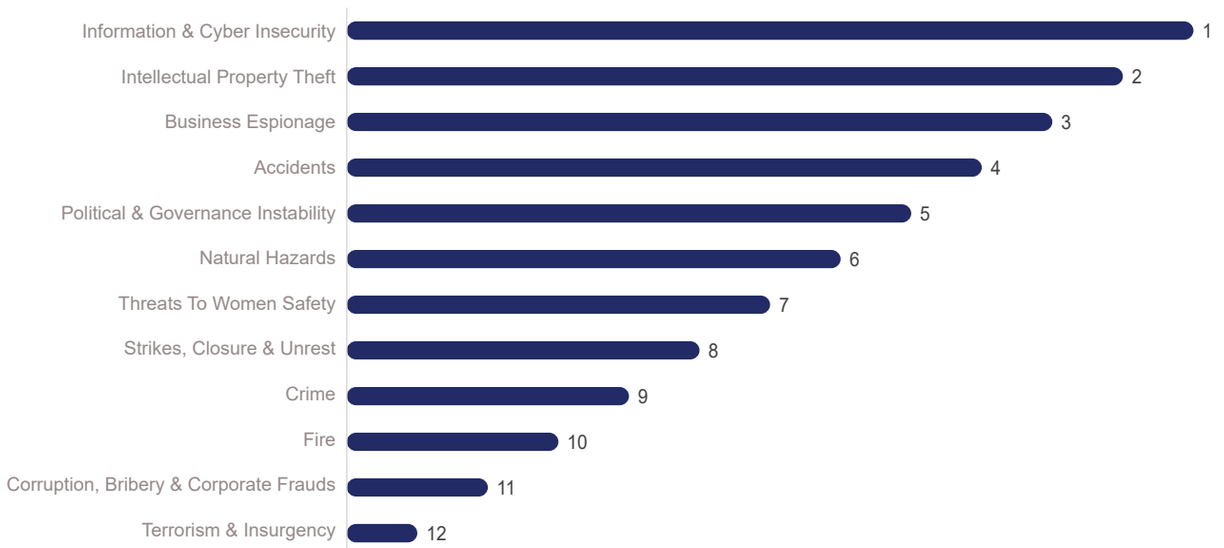
[11] https://www.cioandleader.com/article/2022/01/14/rise-cyber-espionage-india-2022-report

[12] https://www.thehindubusinessline.com/blink/know/booming-business-of-corporate-espionage/article7035984.ece

[13] https://www.shethepeople.tv/news/crimes-against-women-in-2022-ncw/

REGION-WISE RISK RANKING

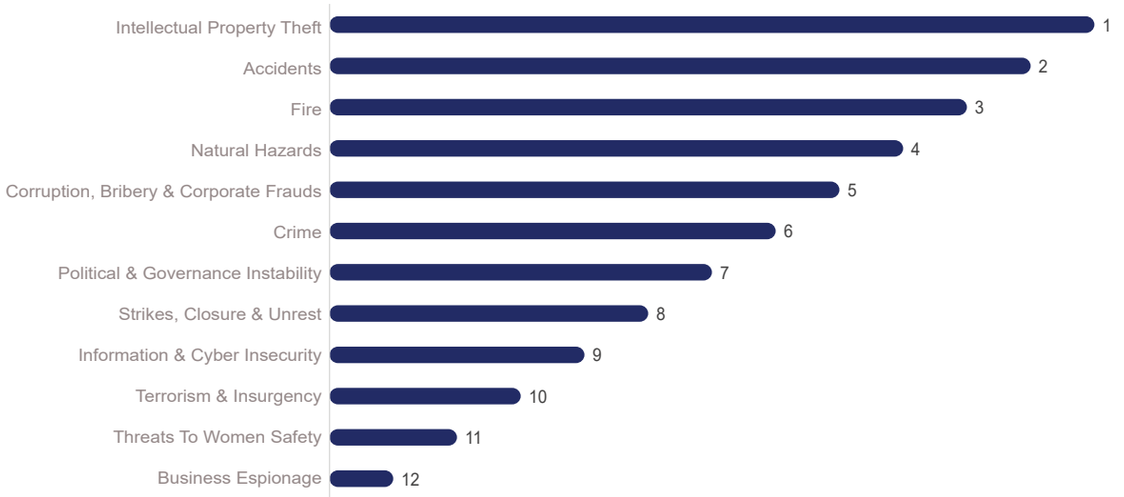
RISK RANKING BASIS RESPONDENTS OPERATING FROM MULTIPLE LOCATIONS IN INDIA



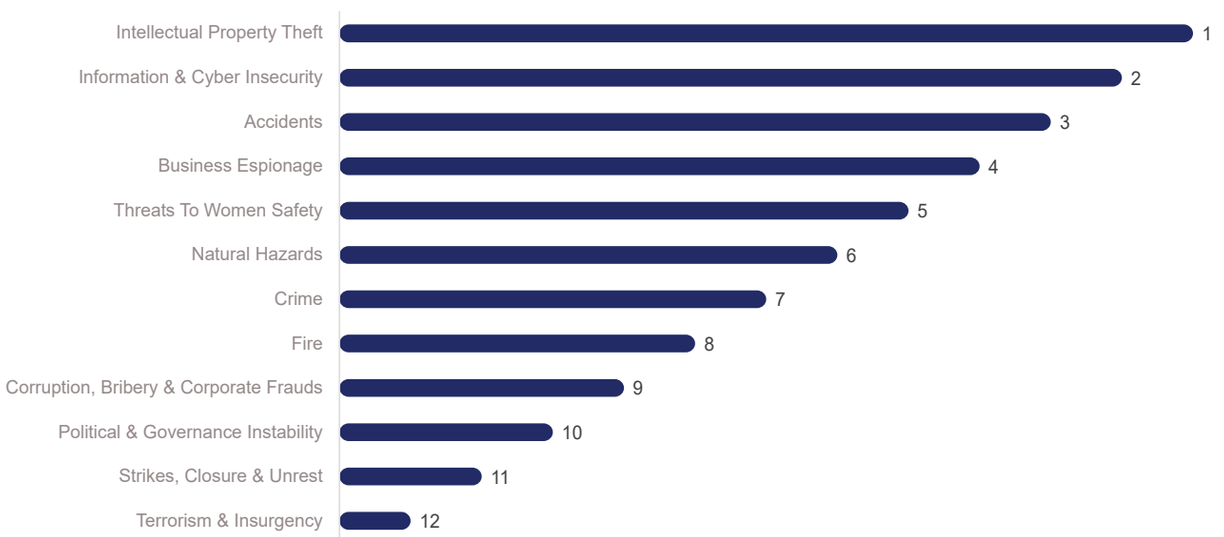
The IRS 2022 survey's respondents state that "Information & Cyber Insecurity" is the top concern for firms operating from different locations in India. The expeditious digitalization of organizations and the online storage of data, both of which have put the security of sensitive data at risk.

Following this risk is "Intellectual Property Theft," which occurs as a result of the competitive corporate environment and competitors stealing trade secrets for their own commercial gain. "Business Espionage" and "Accidents" come in third, fourth, and fifth position respectively.

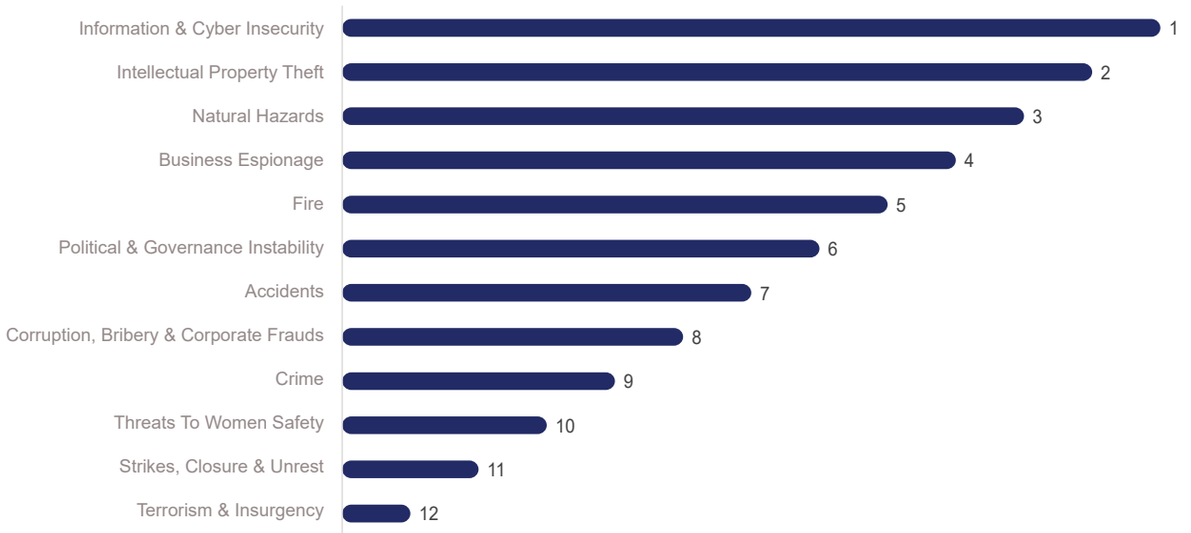
RISK RANKING – BASIS RESPONDENTS OPERATING FROM THE EASTERN REGION



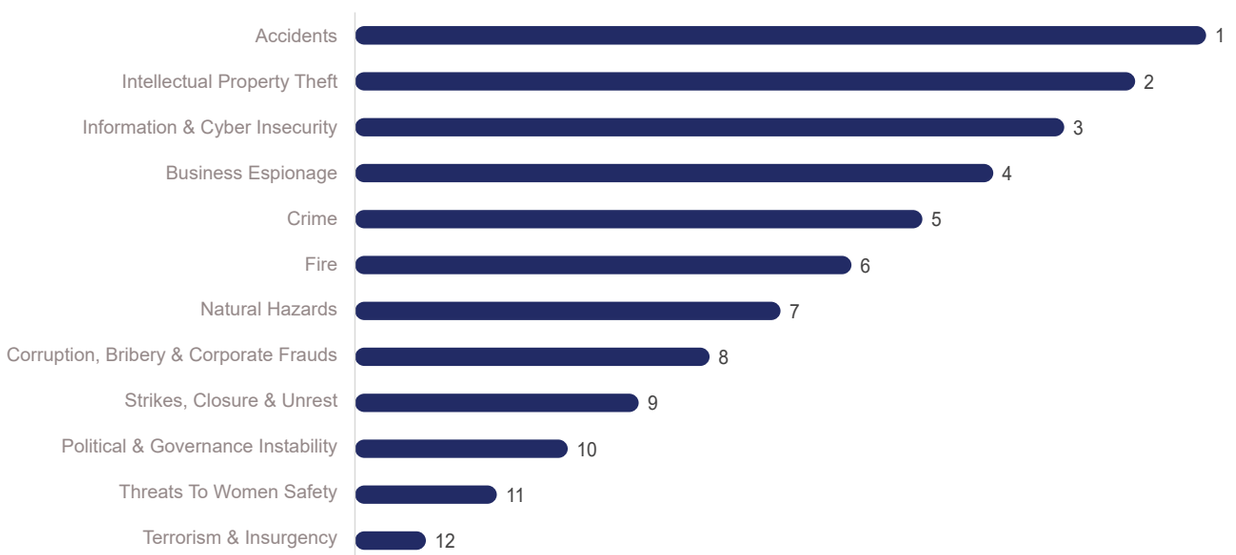
RISK RANKING – BASIS RESPONDENTS OPERATING FROM THE WESTERN REGION



RISK RANKING – BASIS RESPONDENTS OPERATING FROM THE NORTHERN REGION



RISK RANKING – BASIS RESPONDENTS OPERATING FROM THE SOUTHERN REGION



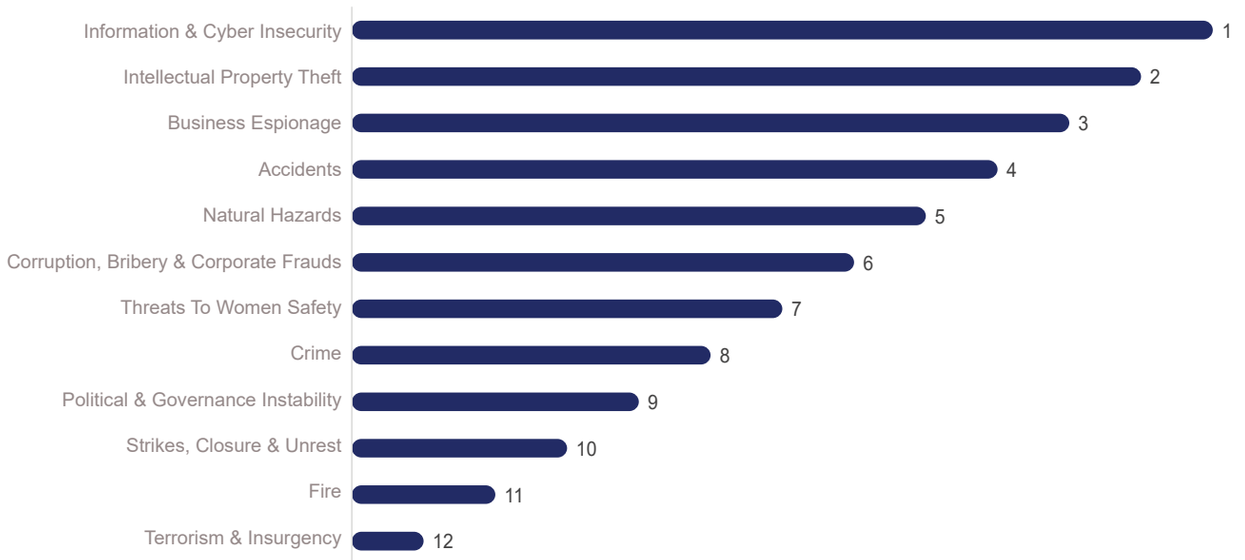
The two biggest challenges to enterprises in the East have been recognized as “Intellectual Property Theft” and “Accidents,” respectively.

The two top risks for the West region have been ranked as “Intellectual Property Theft” and “Information & Cyber Insecurity,” respectively.

“Intellectual Property Theft” has been ranked as the top risk for organizations residing in the North, and “Information & Cyber Insecurity” has been identified as the second-most critical threat.

“Accidents” are the most prevalent risk for the businesses in South, while “Intellectual Property Theft” is the second-most significant disrupting element.

RISK RANKING – BASIS RESPONDENTS OPERATING FROM MULTIPLE LOCATIONS OUTSIDE INDIA

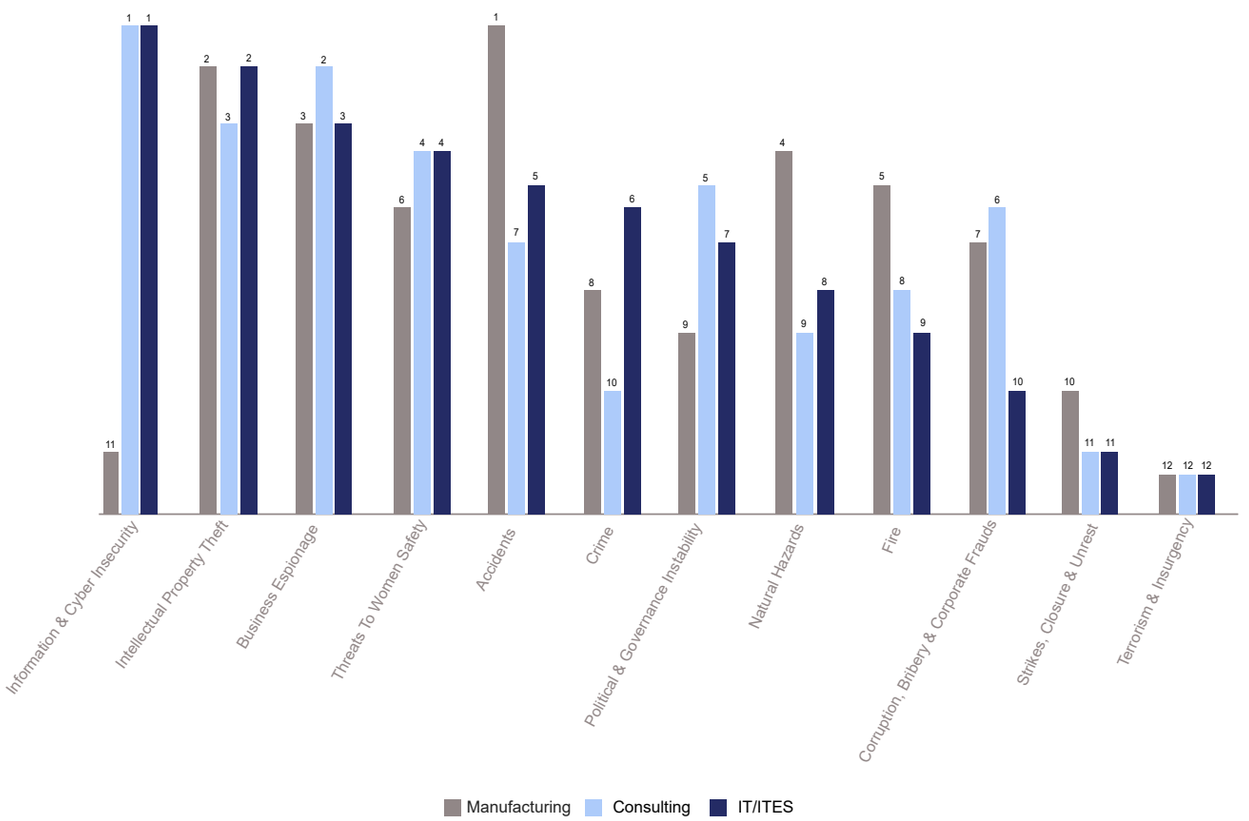


Companies operating from multiple locations outside India have ranked “Information & Cyber Insecurity” as the top risk, with “Intellectual Property Theft” and “Business Espionage” coming in second and third position respectively. These regions include Asia Pacific (APAC), Europe, the Middle East, and Africa (EMEA) and Americas. The respondents ranked “Accidents” and “Natural Hazards” as their fourth and fifth top worries.

INDUSTRY-WISE RISK RANKING

COMPARATIVE PERSPECTIVES ON RISK

RISK RANKING – MANUFACTURING VS. IT/ITES VS. CONSULTING



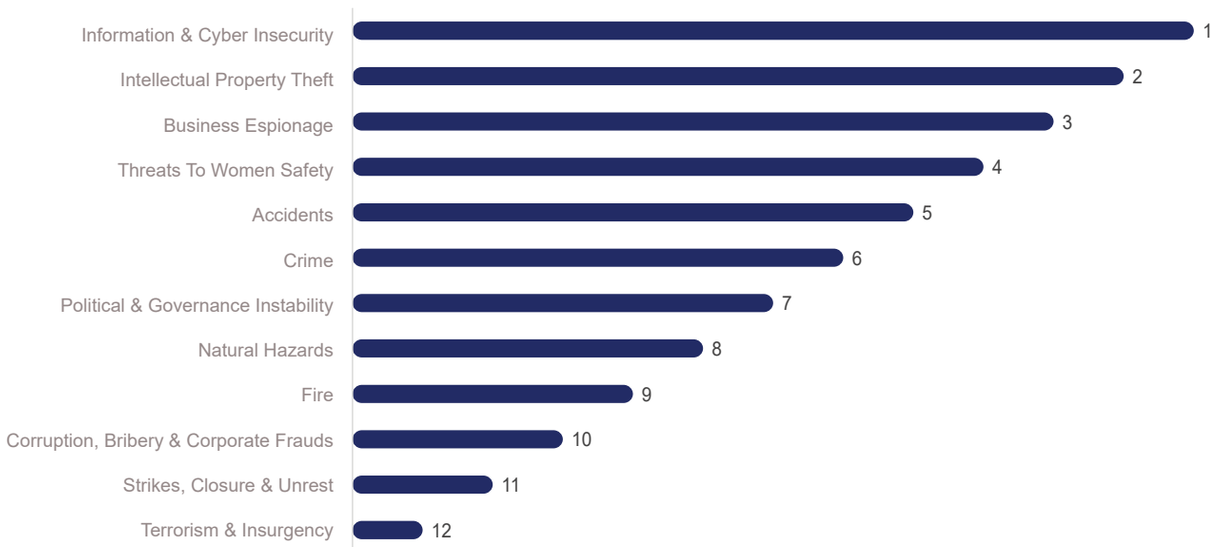
The comparative graph provides an overview of the risk perception for companies in the Manufacturing and Consultancy sectors along with the IT/ITES industry. The impression of threat varies dramatically between the ratings of 12 threats given by each sector. The top risk for the consulting and IT/ITES sectors has been identified as “Information & Cyber Insecurity,” whilst the manufacturing sector’s top risk has been identified as “Accidents.” The other two disruptive threats affecting all three industries are “Business Espionage” and “Intellectual Property Theft.” The growing digitalization and hybrid working paradigm have put data security for each of these areas at

risk, according to the voting patterns of respondents.

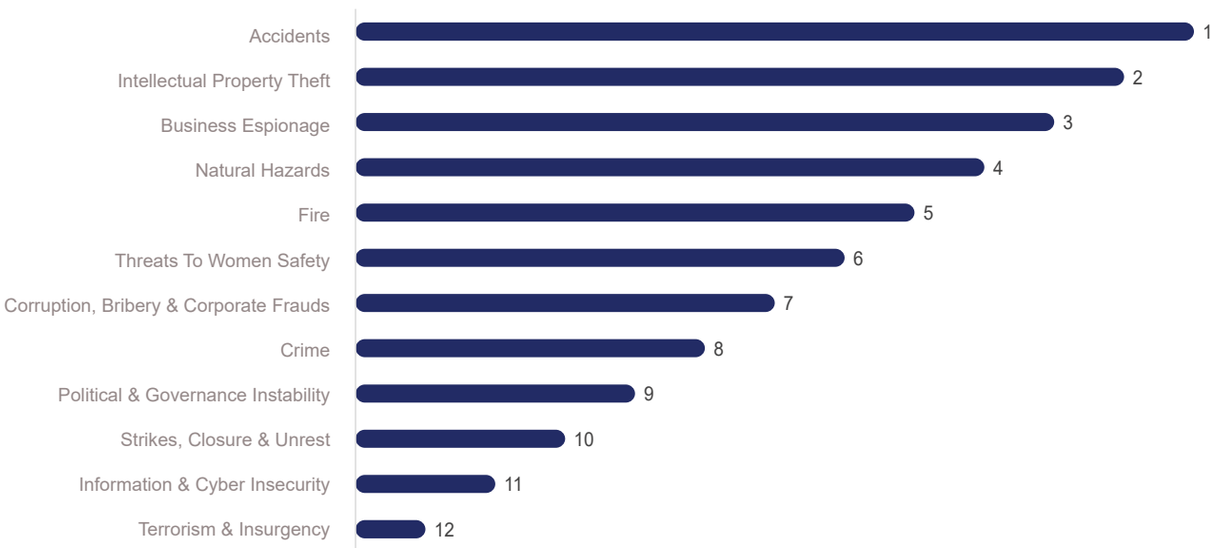
As the world becomes increasingly digital, so do the threats posed to businesses' information and technological infrastructure. The recent survey revealed that respondents are concerned about the possibility of information & cyber insecurity and are actively attempting to improve their security protocols.

India's manufacturing sector started operating again in full swing, which has made it more prone to "Accidents". IT/ ITES and Manufacturing industry has identified "Intellectual Property Theft" as the second most top risk, while the Consulting sector has placed "Business Espionage" in the second spot. For the IT sector, "Business Espionage" and "Threats to Women's Safety" are the third and fourth disruptive factors, "Business Espionage" and "Natural Hazards" have been identified by the Manufacturing sector for the same spots. For Consulting sector, "Intellectual Property Theft" and "Threats to Women Safety" ranked third and fourth, respectively. Accidents, which stand in the top spot in the Manufacturing sector, fall to the fifth spot in the IT sector, while the Manufacturing sector votes for "Fire" as the fifth risk, and Consulting sector has voted for "Political & Governance Instability" at the same spot.

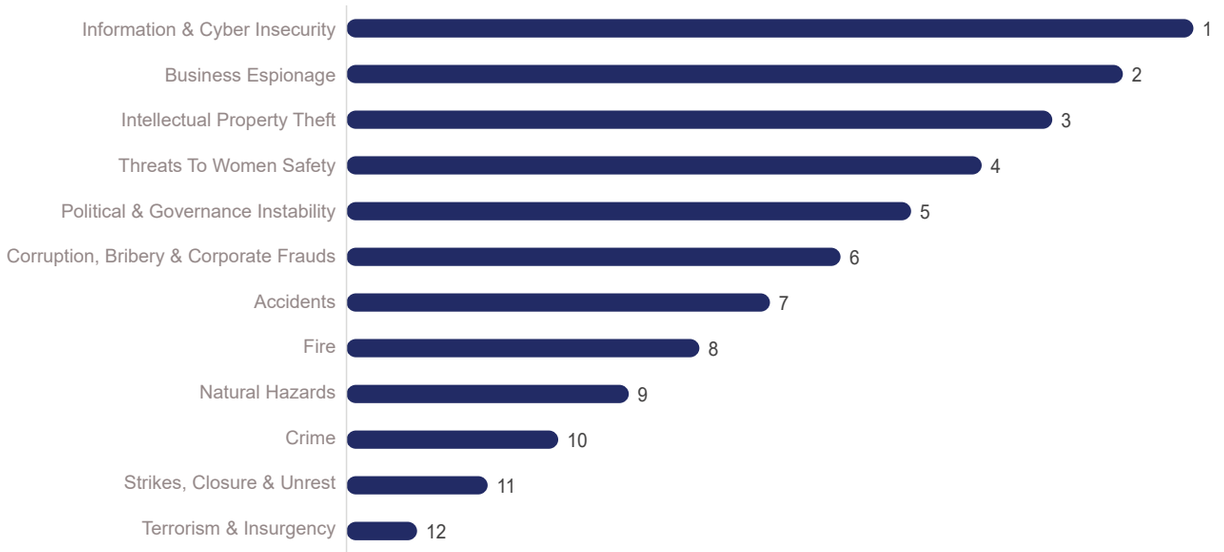
RISK RANKING - IT/ITES



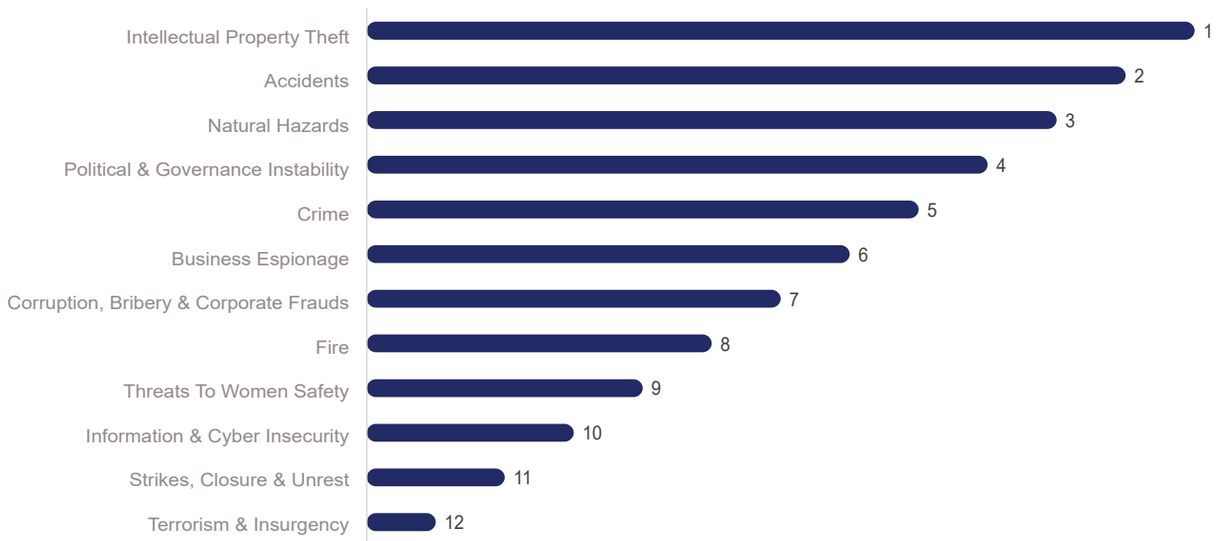
RISK RANKING - MANUFACTURING



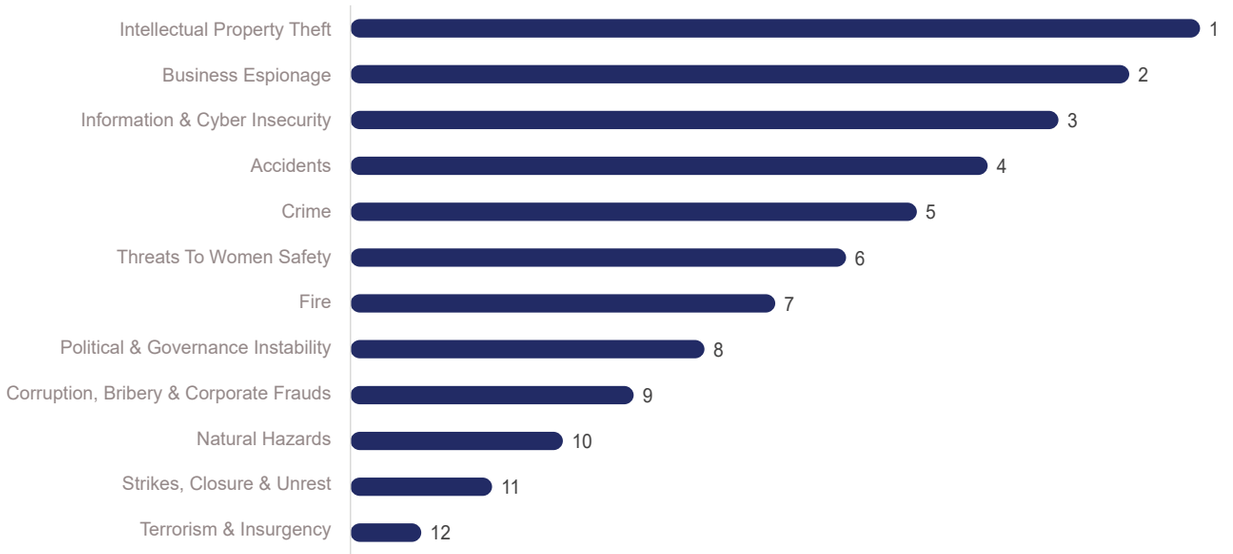
RISK RANKING - CONSULTING



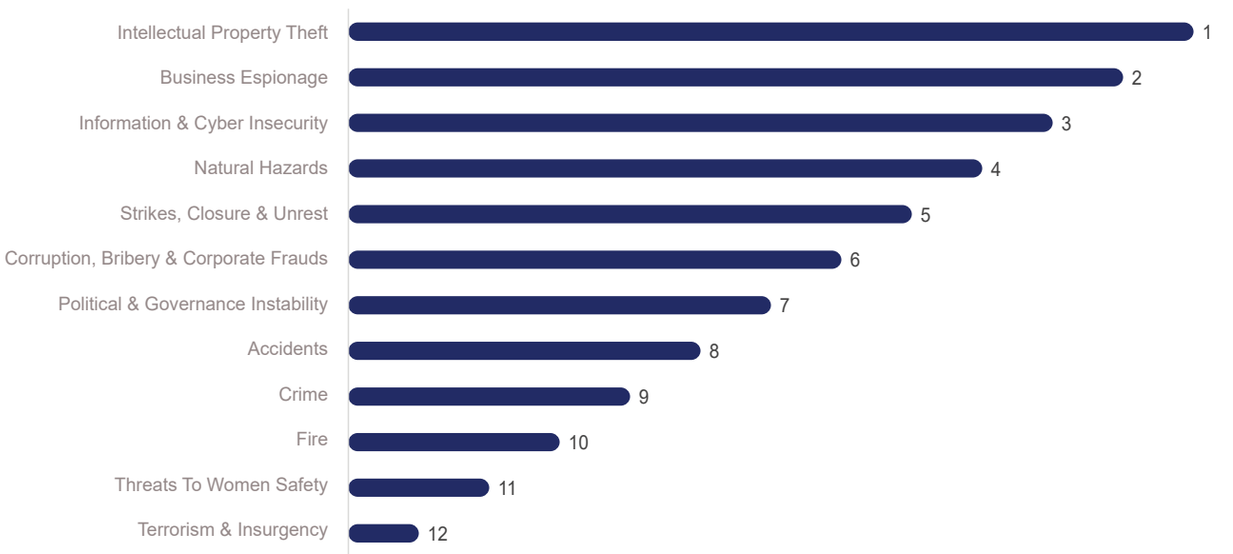
RISK RANKING - REAL ESTATE



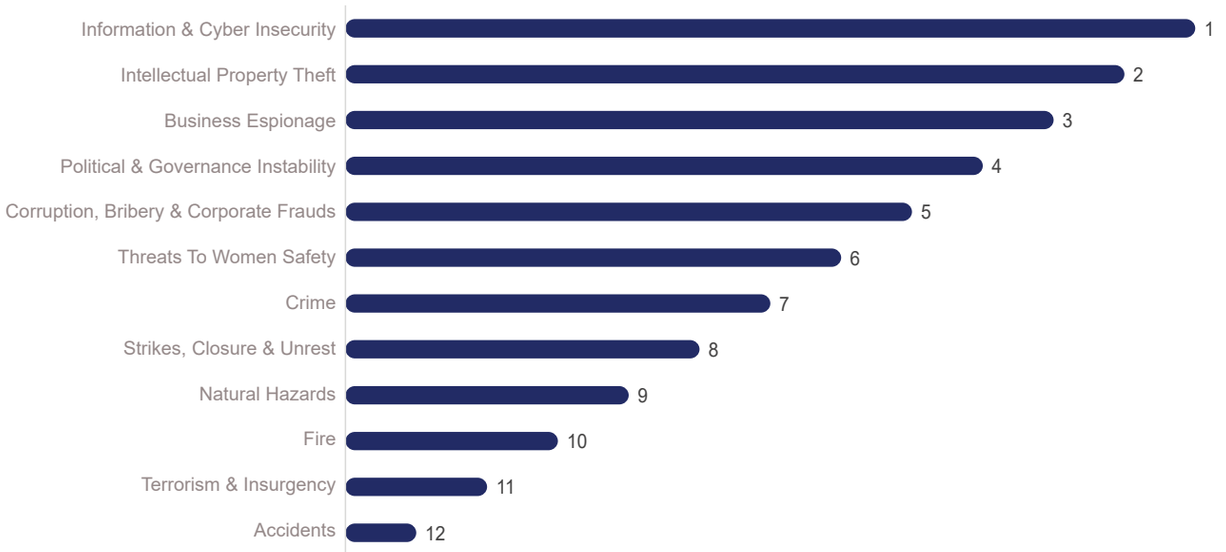
RISK RANKING - EDUCATION



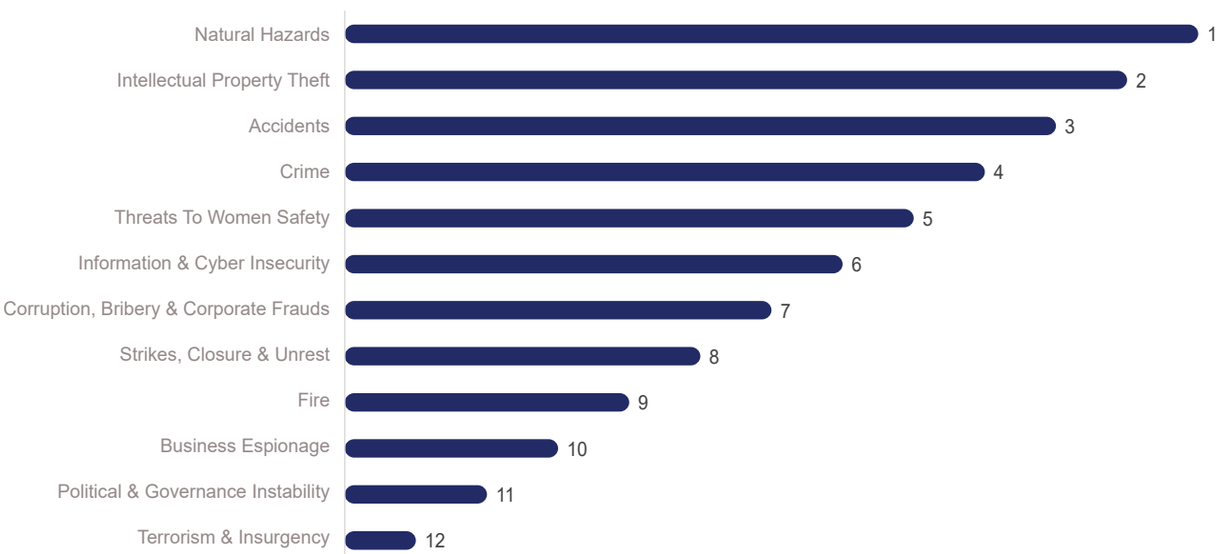
RISK RANKING - SECURITY SERVICES & SOLUTIONS



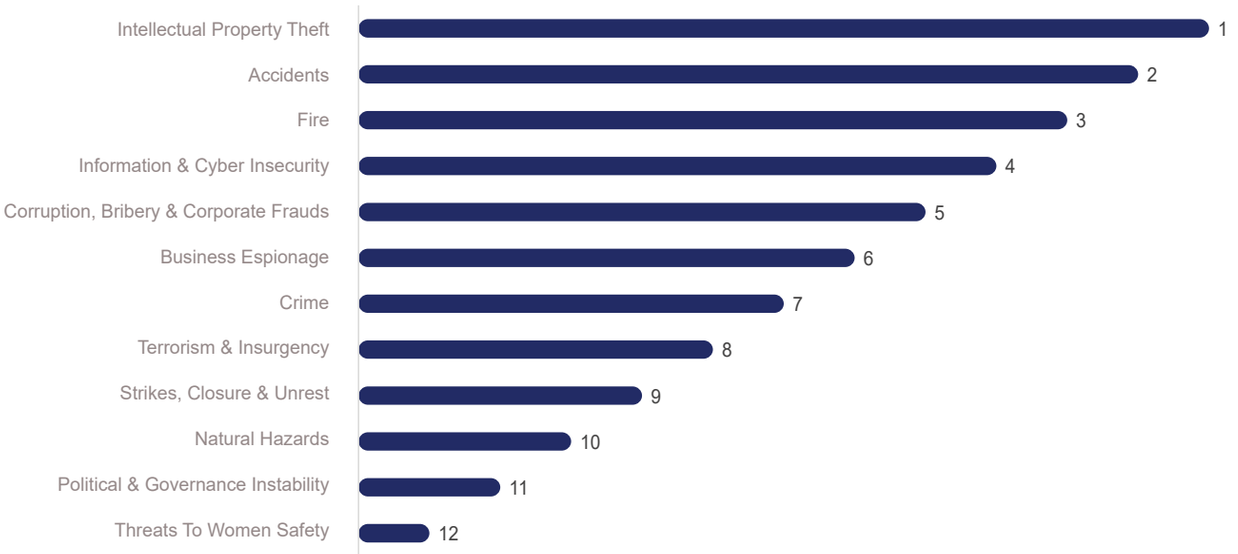
RISK RANKING - FINANCIAL SERVICES



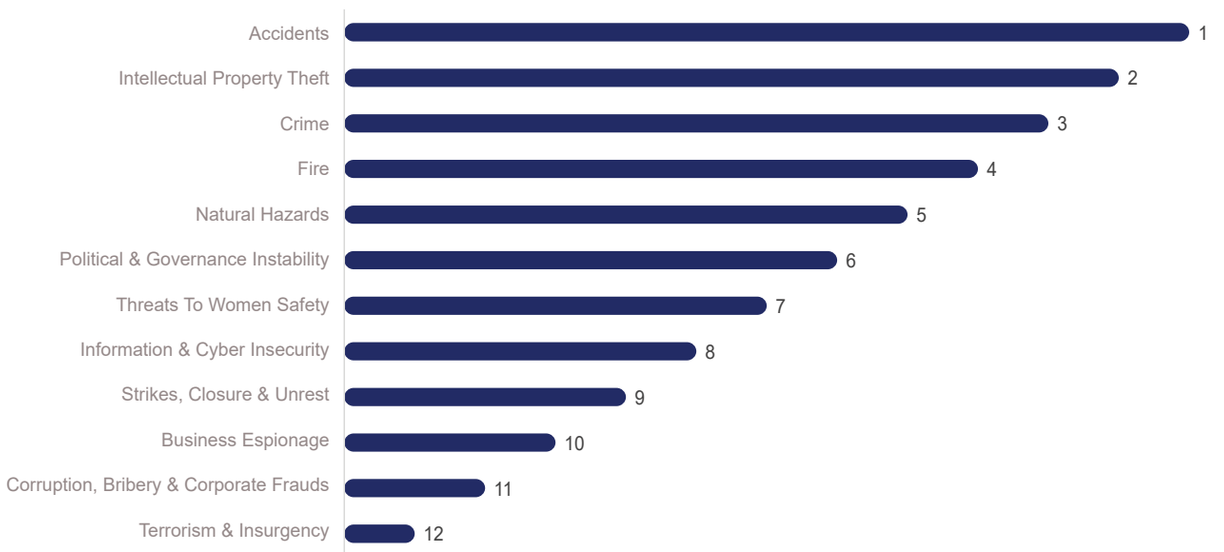
RISK RANKING - HOSPITALITY



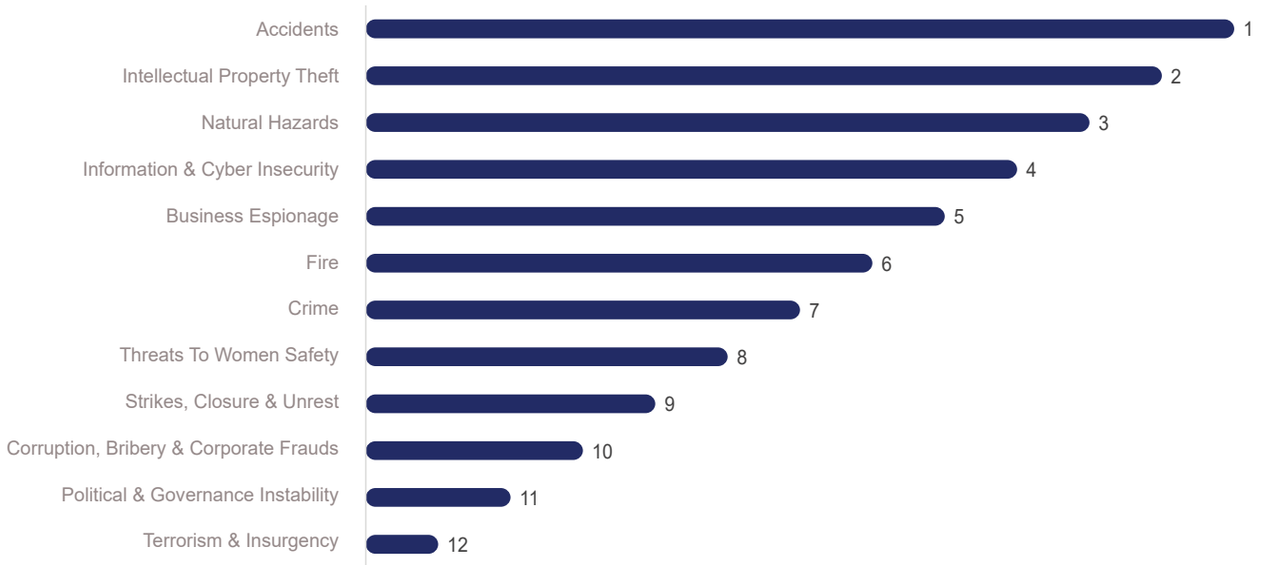
RISK RANKING - LOGISTICS



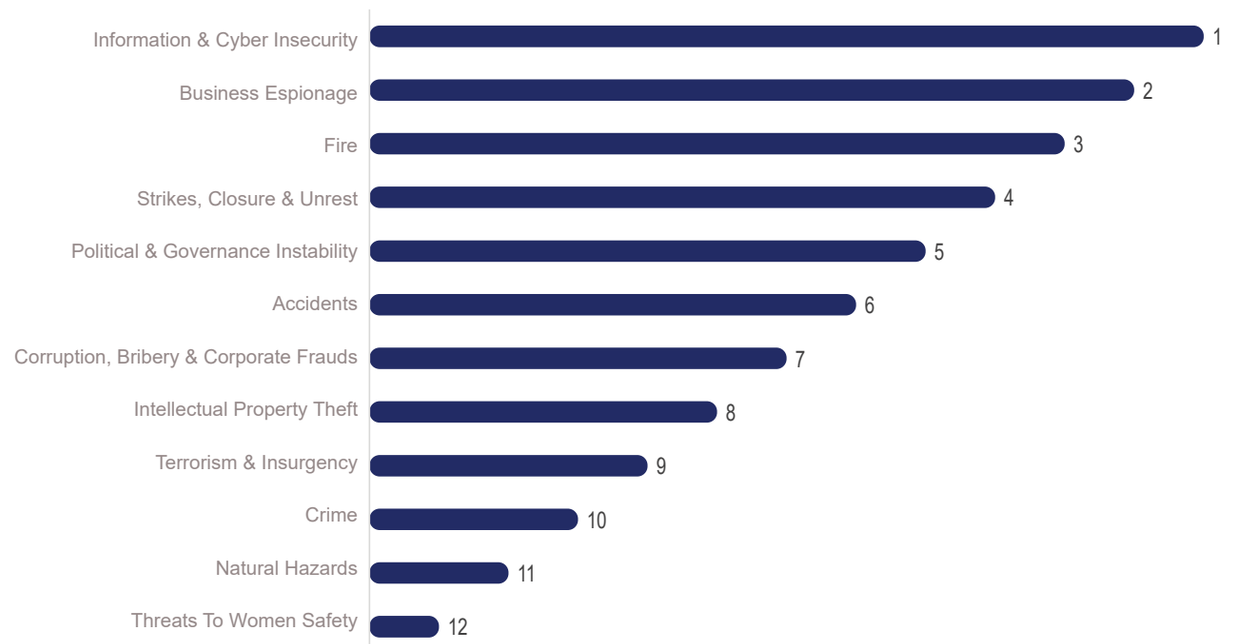
RISK RANKING - CONSTRUCTION



RISK RANKING - RETAIL



RISK RANKING - MEDIA & ENTERTAINMENT



The graphs up top show the risk category rankings according to industry. They differ from one another because each of them has varying degrees of exposure to each risk category and varying amounts of desire to mitigate it.

“Intellectual Property Theft” and “Information & Cyber Insecurity” are occurring in the top 5 places in the majority

of sectors due to the growing digitization and the culture of working from home.

For practically every sector, “Accidents” and “Business Espionage” are also in the top five.

The IT/ITES Sector has voted “Information & Cyber Insecurity, “Intellectual Property Theft” and “Business Espionage” as the most dreadful threats to their business as the cyberattack or intellectual theft might seriously harm or impair their business. The anticipated expenses, such as those related to warning and protecting impacted customers, prospective legal action, and required cybersecurity upgrades, can potentially have more serious effects that may be hidden beneath the surface.

For the Manufacturing Sector, “Accident” is the foremost concern as the factory sites and industries are more prone to accidents which can cause drastic losses to the business.

Consulting Sector has ranked “Information & Cyber Insecurity” as the most disturbing threat followed by “Business Espionage” and “Intellectual Property Theft”. While the Education industry has voted “Intellectual Property Theft” as their biggest concern, then “Business Espionage” and “Information & Cyber Insecurity” respectively.
Both Security Services & Solutions and Financial Services Industries have voted “Intellectual Property Theft”, “Information & Cyber Insecurity” and “Business Espionage” as their top three concerns.
The Hospitality Industry has voted “Natural Hazards” and “Intellectual Property Theft” as their major concern while the concerning threats ranked by the Real Estate Sector is “Intellectual Property Theft” and “Accidents.”

For the Logistic Sector, “Accident” is their second major concern as transportation is more prone to road accidents, while “Intellectual Property Theft” has been placed at 1 by the respondents. Likewise, the Construction Industry has voted “Accidents” on the top position as the construction sites face a lot of challenges in combating accidents.
The Retail Industry has also ranked “Accidents”, “Intellectual Property Theft” and “Natural Hazards” as their prime troubles.
Media and Entertainment Industry has marked “Information & Cyber Insecurity” as a huge threat followed by “Business Espionage” and “Fire”.

Risk Management has always been an important part of the senior management profile, but it has become even more significant in the post covid era. The pandemic has highlighted the need for companies to be more agile in adapting to the changing environment. This is evident in the way many businesses have transformed their operations. Organizations are paying close attention to the possible risks they might encounter, both from a short term and long-term perspective. Industry bodies are also becoming increasingly important. Businesses are now focusing on predicting future scenarios and having a proactive approach to ascertain potential risks and ways to counter the same. From a Publishing and Education Industry perspective, I believe the biggest risk for us has been around Intellectual Property rights, piracy and rising costs. I shall cover each one in more detail and highlight their importance for the industry.

In terms of Intellectual Property rights, copyright laws have always been an area of concern. Copyright infringement is rampant and the strides in the digital space have further compounded this risk. In any industry, I believe the rights of content creators are of paramount importance and their content must be protected at all costs. This not only results in overall growth of the industry but also encourages more content creation and building a strong knowledge economy. In the light of this, legislative amendments are both necessary and urgently needed. These laws were created long back, and the changing business landscape necessitates that we re-look at them with a fresh pair of eyes.

Piracy, both print and digital, is the second major risk for the Publishing/ Education Industry. Over time, piracy has evolved and taken new forms. From books being sold at local bazaars and traffic signals, piracy has become more structured with pirated copies being sold on e-commerce platforms. Digital piracy is also becoming a significant risk for the industry as PDF copies of leading books are being circulated on Whatsapp groups.

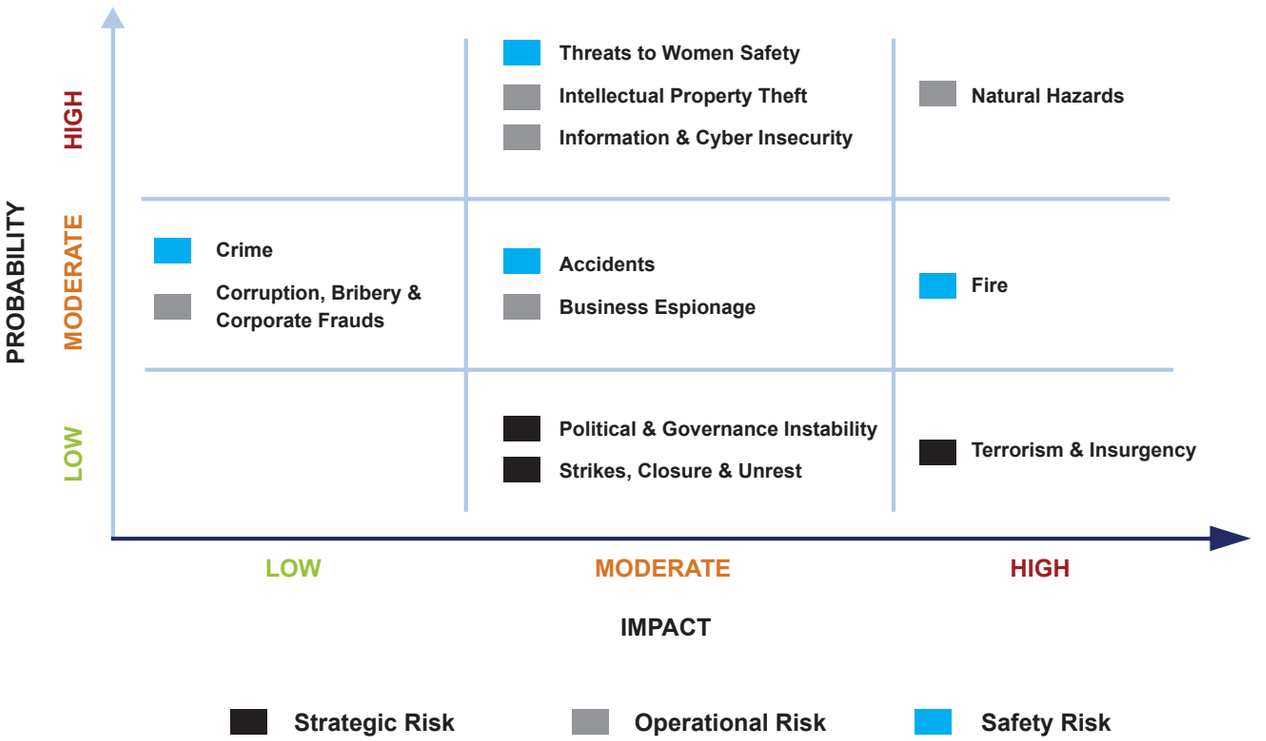
The third major risk is rising costs. These costs are a combination of several developments from the past few years. These include GST, import duty cost and the rising cost of paper. GST on all the inputs used by publishing with no provision of input credits of GST as the final product is non-taxable. The rising cost of paper is a clear case of demand exceeding the supply. All of these factors have led to a consistent increase in costs. These rising costs are of concern as there is a limit to the hit consumers can take.

If the Publishing industry is adequately supported in risks, we can work together with the government to make the dream of having a strong reading and learning society into a reality.

Addressal of these points would not only help every segment of society in sourcing new books and increasing domestic consumption, but also help in establishing India as the Publishing Hub for global consumption.

Mr Neeraj Jain
Chair – FICCI Publishing Committee and
Managing Director, Scholastic India

Risk Categorization



Strategic, operational, and safety risks are the three areas into which risks are classified by the IRS 2022. Strategic risks are those that have a direct impact on an organization's ability to achieve its corporate goals. These hazards seriously affect national security and its ability to survive globally. The organization's top leadership mostly determines strategic risks.

Operational risk is the likelihood of a loss resulting from a failure in an organization's internal controls, operations, or procedures. Finally, safety risks are those that may have an impact on employee safety. They could be internal, external, or both. Since employees are a company's most important asset, any danger to their safety could impact business continuity. A specific risk that comes within the Strategic, Operational, or Safety hazards categories is depicted in the graph on "Risk Category." Their probability and impact demonstrate the severity of these risks to the corporate sector.

Safety risks, such as accidents, crime, and fires, fall under the moderate probability category, but they can have varying impacts, with fires having the highest potential impact, accidents having moderate impact and crime depicting the least impact. Operational risks, such as natural hazards, intellectual property theft, and information & cyber insecurity, are likely to have high occurrences and can have moderate to high impacts on the business ecosystem. Business espionage is also an operational risk, but with a lower probability of occurrence and moderate impact. Corruption, bribery, and corporate frauds also fall under this category with a probability of moderate risk and the lowest impact. Strategic risks such as political & governance instability, strikes, closures, & unrest, have a low probability of occurrence but can have a moderate impact. Terrorism & insurgency is a strategic risk with the lowest probability of occurrence but with the potential for high impact. Safety risks, such as threats to women's safety will have high occurrence and can have a moderate impact. Businesses must evaluate the risks they face, their probability of occurrence, and their potential impact, to develop effective risk management strategies to mitigate them.

Risk in Detail

INTELLECTUAL PROPERTY THEFT



YEAR-ON-YEAR RANKING: Intellectual Property or IP has a significant economic impact on both the national and state economies. Several sectors of our economy depend on the proper protection of their patents, trademarks, and copyrights. However, with the broadening of the competitive landscape, Intellectual Property Theft has been increasing. It has become a serious threat to the business because it can lead to lost sales and revenue, and it can also damage the business's reputation. Thus, the respondents of IRS 2022 have ranked "Intellectual Property Theft" as their top concern, at the 1st position. In the most recent index of international intellectual property rights India dropped from the 40th position it held in 2021 to the 43rd position in 2022.[14]

COUNTERFEIT GOODS: Counterfeit goods refer to fake, unauthorized, and illegally manufactured products. Counterfeit goods harm businesses by imitating the genuine product and undermining the brand's reputation. Counterfeit goods can harm consumers and result in loss of revenue, legal battles, and a tarnished image for the business. Counterfeit goods also impact the economy, leading to job loss and loss of tax revenue. Hence, companies must be vigilant and adopt measures to combat the problem of counterfeit goods to safeguard their brand reputation and ensure the safety of their consumers.

> **'Over the years, Illicit trade has undeniably become one of the greatest risks globally causing economic damage, undermining investments and creating an unequal playing field for the legitimate businesses. It also causes additional risks to citizens, impacting their health and safety, besides fomenting crime, generating black money and funding devastating terror groups. Regardless of different approaches to contain this complex issue, it continues to pummel nations at different levels.**
>
> **Therefore, large scale awareness generation and sustained coordinated efforts, across countries and governments are imperative to address this threat effectively.'**
>
> — **Mr. Anil Rajput,**
> Chairman, FICCI CASCADE and Member-Corporate Management Committee & President, Corporate Affairs, ITC Ltd.

PATENT & TRADEMARK INFRINGEMENT: Patent and trademark infringement occurs when someone uses a patented or trademarked product without the owner's permission. Patent infringement harms

[14] https://www.business-standard.com/article/current-affairs/india-slips-to-43rd-rank-in-us-intellectual-property-rights-index-123022401216_1.html

businesses as it reduces the incentive for businesses to innovate, negatively affects their revenue, and puts them at a disadvantage compared to their competitors. Trademark infringement can also harm businesses by confusing customers, leading to diminished brand value and revenue loss. Therefore, businesses must protect their intellectual property rights by obtaining patents and trademarks and enforcing them through legal action.

IP LEGAL FRAMEWORK: Intellectual property (IP) refers to creations of the mind, such as inventions, literary and artistic works, and symbols. IP legal framework provides a set of laws that protect the creator's rights over their creations. The IP legal framework affects businesses by encouraging innovation, protecting ideas and inventions, and supporting growth. A strong IP legal framework gives businesses a competitive edge, attracts investment, and creates job opportunities. Businesses must clearly understand the IP legal framework and take measures to protect their intellectual property from succeeding in today's competitive market.

INCIDENT MAPPING: The world economy is becoming more interconnected and innovation-driven, fuelled mostly by creativity and intellectual property (IP). According to many business owners, investors, and entrepreneurs, innovations' lifeblood is the trademark. Worldwide intellectual property theft is now a serious concern as intellectual property becomes a battlefield between major economic forces around the Globe. The Indian government has been actively working towards establishing the country as a prominent hub for the development and manufacturing of advanced technologies. Through various international collaborations and initiatives, the government is striving to build trust in the Make in India campaign and strengthen the country's intellectual property ecosystem. The efforts put in by the government are aimed at promoting innovation, encouraging research and development, and creating an environment that fosters the growth of cutting-edge technologies. By focusing on building a robust manufacturing base and promoting indigenous innovation, the Indian government is taking bold steps towards achieving its vision of a self-reliant and technologically advanced nation. These initiatives are expected to attract investment and create employment opportunities, thereby boosting the overall economic growth of the country.

IMPACT AND COMBAT: The Delhi High Court established the Intellectual Property Division (IPD) in July 2021 specifically to hear IPR cases, including those previously heard by the IPAB. Three judges have just been appointed by the Delhi High Court to serve solely as the IPD. The court announced its procedures for handling patent lawsuits simultaneously. According to the April 2022 Parliamentary Committee Report, the Indian Government should urge High Courts nationwide to create their own IPDs.

The Government of India also launched a scheme for facilitating Startups Intellectual Property Protection (SIPP) initiative in January 2016 to help startups protect their Intellectual Property Rights (IPR) in India. The SIPP scheme aims to support startups in securing their patents and trademarks by providing them with financial assistance in the form of reimbursements for the expenses incurred during the filing process. The SIPP scheme reimburses up to 80% of the cost startups incur when filing patents or trademarks. This financial assistance makes it easier for startups to obtain IPR protection and reduces the financial burden associated with the process. The scheme enables startups to expedite securing their patents or trademarks. It allows startups to request expedited processing of their applications, which can significantly reduce the waiting time for obtaining IPR protection. The SIPP scheme also provides startups with legal assistance and support for drafting and filing patent or trademark applications. This support ensures that startups can easily navigate the complex process of securing their IPRs.[15]

Companies that engage in IP infringement suffer from diminished incentives to develop due to the possibility of theft, lost revenue, increased expenses of IP protection, harm to brands, and other factors. When consumers purchase lower-quality counterfeit products, such as fake pharmaceuticals, they put their health and safety at risk. Governments incur expenditures for enforcement as well as lost tax revenue. IP infringement reduces the incentives for innovation, which weakens the country's competitiveness and hinders job growth. Intellectual property theft from overseas hurts companies by increasing costs, decreasing revenue, and eroding profitability. Pharmaceutical and automotive counterfeits can put consumers at risk for health or safety, while pirated software can compromise computer security and violate personal privacy.[16]

[15] https://www.vccircle.com/whythe-govt-should-extend-the-ipr-scheme-for-startups

[16] https://stratnewsglobal.com/trade-tech/china-leads-in-theft-of-u-s-intellectual-property-india-on-priority-watch-list/

RISK OF IP THEFT TO BUSINESSES IN INDIA – AND INDIA'S DRIVE TO COMBAT IT

India has some of the most favorable conditions for businesses to thrive, and as such, a large number of international businesses have set up shops in India over the last few years. In fact, the influx of businesses in India have seen a boom since Covid-19, with major brands like Apple expanding their footprint greatly.

One of the factors which attract businesses to India is the robust intellectual property legal ecosystem in India. For instance, patents in India can be granted as fast as 7-8 months! Trademarks (in case of straightforward cases) can get registered as fast as 5-6 months. Moreover, courts in India have also evolved greatly over the years, when it comes to the handling of IPR cases.

IP Theft Problems Faced By Various Industries

FICCI in collaboration with Pinkerton had released a very illuminating report in 2021 (India Risk Survey Report) which identified Intellectual Property Theft as one of the top-3 concerns for businesses in India. In this context, given the high importance given by businesses to IP theft concerns in India, it is first important to identify the various kinds of IP theft risks, in an industry-specific manner.[17] In this regard, the below (non-exhaustive) table can be utilized to understand the various IP risks in different industries:

S.No.	Industry	IP Theft Concerns
1	Publishing	Large-scale sale of counterfeits; Availability of counterfeits on e-commerce portals; Printers and photocopiers disseminating counterfeits on a large scale; Problem of copyright – many rights holders do not possess requisite copyright registrations, and in India, having a copyright registration is very helpful in legal proceedings (even though copyright registration is not mandatory.
2	OTTs and Live Sports	Piracy; Circumvention of software protections; Problems in tracking source; Mirror websites;
3	Hospitality & F&B	Infringement/ misuse of house marks (in our experience, there are innumerable hotels and restaurants operating in India, whose names are clear infringements of the names of other brands;
4	Pharmaceuticals	Counterfeiting;

[17] https://ficci.in/India-Risk-Survey-2021-Report.pdf

S.No.	Industry	IP Theft Concerns
5	Information Technology	Software Piracy;
6	Manufacturing	Supply chain breaks – counterfeiting; Counterfeiting of parts;
7	Education	Counterfeiting of study material; Fraud and misrepresentation – misuse of trademarks by unauthorized persons;
8	Security Services & Solution Providers	Infringement of trade names; Fraud and misrepresentation by using IP;
9	Automobiles	Spare Parts – counterfeiting; Unauthorized service centers – making unauthorized use of trade names and marks;
10	E-commerce	Sale of counterfeits on e-commerce;

Important Steps To Detect And Combat IP Theft Risks

While the above risks may seem daunting, there are a few simple steps that all IP rights holders should do to not only combat IP theft risks but also increase the prospects of their own businesses in India:

- **Due Diligence – investigations to identify the risks and the parties/ persons involved;**
- **Identifying major players in the market – prioritizing targets for enforcement and anti-counterfeiting activities;**
- **IP audits of infringers/ counterfeits to check if they have applied for their own IP;**
- **Securing supply chains;**
- **Identifying online infringements/ counterfeits available online, for crackdown;**

PROACTIVITY OF THE INDIAN IPR ECOSYSTEM TO MITIGATE AND COMBAT IP THEFT RISKS

As mentioned above, the unprecedented use of technology has catalysed risks of IP theft for various industries by manifold. However, these troubled circumstances and their repercussions have been taken note of and in the last few years, several significant reforms and developments have taken place in the Indian legal system as well as the approach of the judiciary towards IPR cases, which has greatly improved the system and practice in-place to combat IP theft. A few notable examples of the same are explained below:

The establishment of Intellectual Property Division in Delhi and Madras

Pursuant to the abolishment of Intellectual Property Appellate Board (IPAB) in 2021, the establishment of Intellectual Property Division was announced in the High Court of Delhi in 2022, and now very recently in the High Court of Madras. [18]

[18] https://ssrana.in/articles/ip-division-madras-high-court-directions/

The creation of a specific Bench dealing with adjudication and enforcement of IPR cases only ensures a uniformity and consistency in enforcement of IPR rights. Post establishment, the IPD of the Hon'ble Delhi High Court has pronounced notable judgments in the realm of IP protection and enforcement which reflects that the Indian Courts have become proactive and the recent trends in award of punitive damages also show the stringent behaviour of Courts against counterfeiting.

Enhanced Punitive Damages against Counterfeiting

Some recent cases unveil as to how the Indian Judiciary has embraced a firmer approach when it comes to counterfeiting and awarded damages which will act as a deterrent on counterfeiters.

In the case of Adidas Ag & Anr. v. Praveen Kumar & Ors.[19], the Plaintiff alleged that the Defendants' had infringed its Three striped mark. The Defendant in the case was found with 384 pairs of counterfeit Adidas shoes. Photographs of the Defendant's premises also showed that Defendant was selling a large variety of shoes under various brands using the 'THREE STRIPES' device mark. Subsequently, the Hon'ble High Court of Delhi held that under the circumstances of the case, damages were liable to be awarded against the Defendant and directed the Defendant to pay INR 20 lakhs in damages.

In the case of Koninlijke Philips N.V. and Ors. v. Amazestore[20], the Plaintiff alleged piracy of its registered design of beard trimmer and stated that the Defendants' trimmers were an imitation of the shape and configuration of the beard trimmers for which the Plaintiffs' enjoyed the design registration. The Court in view of facts and circumstances of the case, held that the beard trimmers being sold by the Defendants very closely resembled the beard trimmers being sold by the plaintiff and held the Defendants liable for infringement of the registered design of plaintiff and also for infringement of copyright, passing off and unfair competition.

The Court in the case awarded damages to the tune of a whopping INR 3.15 crores (USD 400K approx.) and also provided the formula for calculating damages as under:

Degree of mala fide Conduct	Proportionate award
First-time innocent infringer	Injunction
First-time knowing infringer	Injunction + Partial Costs
Repeated knowing infringer which causes minor impact to the plaintiff	Injunction + Partial Costs + Partial damages
Repeated knowing infringer which causes major impact to the plaintiff	Injunction + Partial Costs + Compensatory damages
Infringement which was deliberate and calculated (Gangster/scam/mafia) + wilful contempt of court	Injunction + Partial Costs + Aggravated damages (Compensatory + additional damages)

[19] CS(COMM) 1269/2018 and I.A. 16629/2018, order dated May 14, 2019

[20] 2019 (78) PTC 618 (Del)

Dynamic Injunctions by Courts

In 2002, the Delhi High Court in the case of Taj Television Ltd. and ors. v. Rajan Mandal and ors.[21] passed its very first 'John Doe order', commonly known in India as an 'Ashok Kumar order'. As the name suggests, John Doe orders are ex-parte orders enforceable against an unknown party. These orders help prohibit any potential infringing activities by unidentified people.

However, these orders were becoming ineffective due to similar 'mirror/ redirect/alphanumeric' websites that cropped up after the original website was taken down and that displayed the same infringing content as the original website. Taking a leap forward, the Delhi High Court on April 10, 2019, through its order in the case of UTV Software Communication Ltd. and ors v. 1337x. To and ors.[22], set down a broad legal framework for blocking websites, by granting, for the first time, the remedy of a 'dynamic injunction'. "Dynamic injunction" was defined by Hon'ble Ms. Justice Pratibha Singh in the UTV case as "an injunction order that is not static but dynamic. This means that, while the initial injunction order may only apply to one website, if mirror websites are created, the injunction will dynamically apply to those mirror websites as well."

Thus, Dynamic injunctions enable the Courts to extend the original injunction order and include the new /additional mirror/fake websites that have the same content as the original one and are only registered under a different domain name and/or use a different IP address.

If a plaintiff obtains a dynamic injunction against certain rouge domain names and/or URLs, it implies that the Plaintiff will not have to approach the Court again if the same content appears on a different domain name or URL; the injunction order blocking the initial domain name or URL will also be applicable to the new domain name or URL.

Several other similar orders of dynamic injunction have been passed by the Indian Judiciary in the recent past. Hence, dynamic injunction is a new type of injunction that helps in combating counterfeiting and piracy and also provides effective remedies to IP right holders.

CONCLUSION

Thus, it is clear that while India does have a myriad of problems vis-à-vis IP theft, the legal ecosystem is also equally proactive in taking steps to counter such problems. For instance, given the recent developments, it will not be surprising if other High Courts also come up their own IP Divisions to specifically deal with IPR cases.

Mr. Vikrant Rana
Managing Director
SS Rana & Co.

[21] CS(OS) No. 1072/2002

[22] Cs (Comm) No. 724/2017

INFORMATION & CYBER INSECURITY



YEAR-ON-YEAR RANKING: According to the India Risk Survey 2022, Information & Cyber Insecurity has held onto its second position as a top issue for organizations in 2022. India has experienced a tremendous shift towards digital technology in practically all areas of public life. More than 900 million people use the internet and 650 million have smart phones in the country.[23] Initiatives like Made in India and Digital India are making a favourable impact on the economy. Although digitalization has helped the Indian economy thrive, it has exposed sensitive data to cybercriminals causing huge losses to businesses.

DATA THEFT, PHISHING AND HACKTIVISM THREATS: Data theft, phishing, and hacktivism are serious threats to businesses that can result in the loss of sensitive information, intellectual property theft, and financial loss. Cybercriminals often carry these threats using advanced tactics and tools to gain access to business networks and steal data. Businesses need to implement security measures such as firewalls, encryption, and two-factor authentication to protect their data from such threats. Training employees on safe online practices can also help reduce the risk of data theft and phishing attacks.

COMPLIANCE AND REGULATORY INCIDENCES: Compliance and regulatory incidences occur when businesses fail to comply with industry regulations and laws. These incidents can result in legal action, fines, and reputational damage. Non-compliance can also lead to the loss of customers, as consumers prefer to do business with companies that follow regulations and are transparent about their operations. To avoid regulatory incidents, businesses must comply with industry regulations, maintain accurate records, and have processes in place to prevent compliance breaches.

DOMAIN-BASED THREATS AND CYBER INFRASTRUCTURE ATTACK: Domain-based threats and cyber infrastructure attacks target business's digital assets, such as their website, email, or server. These attacks can cause significant damage, resulting in downtime, loss of data, and reputational damage. Businesses need to ensure that their cybersecurity measures are up to date and that they regularly test their systems for vulnerabilities. Implementing strong password policies, restricting access to sensitive data, and performing regular backups can help mitigate the risk of cyberinfrastructure attacks.

EXECUTIVE THREATS, IMPERSONATIONS AND SOCIAL MEDIA PERILS: Executive threats, impersonations, and social media perils target individuals within a business, such as executives or employees. These threats can result in identity theft, reputational damage, and financial loss. Businesses need to provide training to employees to help them identify potential threats, such as phishing emails and social engineering tactics. Implementing two-factor authentication, monitoring social media accounts, and using encryption can help protect against these threats. Additionally, businesses should have a clear protocol to handle incidents of impersonation or social media perils.

INCIDENT MAPPING: The new wave of digitalization has changed how business is conducted worldwide. Companies all across the world are embracing tech-driven operations more and more. In recent years, with the increasing use of the internet and digital banking, there has been a significant rise in cyber-attacks and incidents related to cybersecurity in India. This trend has been particularly observed in the government sector, with data accessed by IANS indicating a significant increase in cyber security incidents related to government institutions, particularly in 2022. The data shows that the number of such incidents rose from 48,285 in 2021 and jumped up to 1,92,439 in 2022. These figures highlight the growing threat of cyber-attacks in India and the need for increased cybersecurity measures across all sectors.[24]

India is currently one of the nations that encounter various cyberattacks. Air India announced a cyber-attack in May 2021 that compromised 4.5 million of its customers' data worldwide.[25] One of the five marine facilities in India's largest container gateway, Jawaharlal Nehru Port Container Terminal (JNPCT), suffered a temporary

[23] https://economictimes.indiatimes.com/news/economy/indicators/unique-factors-at-work-to-ensure-india-becomes-3rd-largest-economy/articleshow/98131860.cms?from=mdr

[24] https://www.business-standard.com/article/current-affairs/cyber-security-breaches-are-up-multiple-times-as-internet-penetration-grows-123021900451_1.html

[25] https://www.google.com/amp/s/www.hindustantimes.com/india-news/air-india-data-breach-all-you-need-to-know-101621647788771-amp.html

outage in February 2022 due to a suspected ransomware assault (Nhava Sheva).[26] In addition to significant financial losses, data leaks may expose sensitive user information. In such circumstances, customers risk having their private and confidential information misused. A single data loss incident can significantly impact the public image and prospects for business growth. Yet, 40% of businesses do not have a thorough plan in place to deal with cyberattacks despite these catastrophic repercussions. The new guidelines released by the Ministry of Electronics and Information Technology, according to the Information Technology Act, 2000, are pertinent given this background.[27]

> **In the face of modern-day cyber threats, waiting for an attack to happen is not an option that organizations can afford. Adopting a reactive approach is like inviting the enemy to invade your territory. The key to an effective cyber defence strategy is to be proactive in seeking out potential threats through relentless threat hunting.**
>
> **While threat hunting may seem like a daunting task, it helps the IT security teams identify and address the vulnerabilities before they are exploited by cybercriminals and also minimize the risk of any successful attack if it happens. There's no room for complacency in the rapidly evolving threat landscape, and organizations must be ready to fight back with all their might.**
>
> — **Mr. Praveen Jaiswal**
> Co-Chair—FICCI Homeland Security
> Co-founder, Vehere

IMPACT AND COMBAT: Cybercrime has become a major threat worldwide, with global losses due to such crimes amounting to an average of 2.5% of GDP. India, with its ambitious goal of developing a 5 trillion-dollar economy, faces a significant risk from the potential losses resulting from large-scale cybercrime.[28] The Indian government has been aware of this threat and has been working to improve the country's cybersecurity systems. The central government has been taking measures to ensure that India's cyberspace is safe, secure, reliable, and efficient. By improving cybersecurity, the government aims to minimize the impact of cybercrime on India's economy and protect the sensitive data of individuals, businesses, and government institutions. It is essential for the government to continue investing in cybersecurity to prevent cyber threats from undermining India's economic growth and development.[29]

The types of cybercrime that have the biggest economic impact include the following:

- The theft of Personally Identifiable Information (PII) frequently leads to online fraud, financial crimes, and the loss of intellectual property and business-confidential information.
- Financial trickery aimed at publicly traded firms.
- Opportunity costs include delays in services or manufacturing and diminished confidence in online activity.
- The expense of network security, the cost of cyber insurance, the expense of recovering from cyberattacks, and the liability risk for the affected organization and its brand.

In more than three out of five (64%) firms that encountered an incident during the survey period, cyber security

[26] https://theloadstar.com/ransomware-attack-hits-nhava-sheva-container-terminal/

[27] https://timesofindia.indiatimes.com/blogs/voices/bolstering-cyber-security-in-indian-digital-economy/

[28] https://government.economictimes.indiatimes.com/news/secure-india/indias-dream-of-usd-5-trillion-economy-threatened-by-cybercrime-risks-are-the-systems-in-place-to-tackle-it/98464431

[29] https://government.economictimes.indiatimes.com/news/secure-india/indias-dream-of-usd-5-trillion-economy-threatened-by-cybercrime-risks-are-the-systems-in-place-to-tackle-it/98464431

assaults have also led to job losses across several areas.[30]

To combat these threats, businesses can take several proactive measures:

- Conduct a comprehensive risk assessment: Businesses should identify potential information and cyber security risks and evaluate their likelihood and impact. This assessment should cover all aspects of the business, including technology systems, data handling processes, and employee behaviour.
- Develop and implement security policies and procedures: Businesses should develop security policies and procedures that address identified risks and establish clear guidelines for employees to follow. This includes defining access controls, establishing password policies, and implementing security controls such as firewalls and antivirus software.
- Provide regular security training for employees: Businesses should ensure that all employees receive regular security training to raise awareness of potential threats and reinforce best practices for information and cyber security.
- Monitor and audit systems & processes: Regular monitoring and auditing of systems & processes can help detect potential security breaches or weaknesses and allow businesses to take corrective action before any damage is done.
- Implement incident response plans: Businesses should have an incident response plan in place that outlines the steps to be taken in the event of a security breach. This plan should cover notification procedures, containment measures, and communication protocols.

According to an industry report, 50% of Indian businesses believe they have fully mitigated their cybersecurity risk exposure in numerous crucial areas, even though organizations are increasingly concerned about threats and cyber events. 65% of the executives polled report that the budget grew in 2022 and that they aim to raise their spending on cybersecurity in 2023. Budget increases reflect the reality that cybersecurity is the most important topic for resilience planning.[31]

[30] https://www.dailyexcelsior.com/impact-of-cyber-crimes-on-indian-economy/

[31] https:/www.pwc.in/press-releases/2022/over-82-of-business-executives-in-india-foresee-an-increase-in-cybersecurity-budgets-in-2023-pwc-survey.html

INCREASING RISKS TO ORGANISATIONS DUE TO CYBER THREATS

Introduction:

In today's constantly evolving economic, social, and regulatory environment, the efficacy of traditional corporate cybersecurity measures has come under question.

Due to cloud computing and growing decentralized threats, the methods that were once suitable for securing data, applications, and IT infrastructure when they were contained within a company's premises are no longer adequate. Modern digital organizations operate in a hyperconnected, boundaryless network, which leads to an expanded threat surface and more opportunities for malicious actors to infiltrate and cause harm.

In a report issued by the Data Security Council of India, it was mentioned that approximately 30% of both on-premises and cloud assets have not been inventoried, providing a key advantage for attackers to exploit.[32]

Despite the technology advancements that are enabling enterprises to become more purpose-driven, resilient, and adaptable, many companies still neglect basic cybersecurity principles and tools. Instead, they focus on rapidly introducing new products to the market, which often results in security standards and governance falling behind. This approach leaves important data and critical operations vulnerable to cyber threats.

As per the India Ransomware Report published by CERT-In, there was an overall 51% increase in ransomware incidents reported in 2022 (in the first half of the financial year) compared to the previous year (2021).[33] Unfortunately, this surge in ransomware attacks and other cyber incidents is expected to persist and escalate in the coming years if not handled effectively.

The Current Cybersecurity Landscape:

The cyber threat landscape has undergone a significant transformation in recent years. The primary trends in cybersecurity risks include:

1. **Intellectual property theft: It entails the unlawful acquisition of a company's concepts, innovations, and artistic creations, collectively referred to as "intellectual property."**
2. **Malware attack: Malware encompasses a range of hostile or invasive software and programs. These programs are intended to work against the computer user's desires and are specifically designed to disturb, harm, or gain unauthorized entry to a system.**
3. **Software supply chain attacks: A software supply chain attack aims to exploit vulnerabilities in the software update and supply chain of an organization. These attacks target the trust that organizations have in their third-party vendors, particularly in software updates and patching.**
4. **Industrial IoT technologies hacks: It pertains to hacking, which is the act of modifying or changing software and hardware technology to achieve a goal that falls outside of the creator's initial intention.**
5. **Man-in-the-middle attack: In a Man-in-the-middle attack, attackers intercept the communication between a user and a remote system, breaking the assumption that the communication is direct. By doing this, they can steal credentials, access sensitive data, and manipulate the responses received by the user.**

[32] https://www.dsci.in/content/cybersecurity-consolidation-enabling-competitive-edge-and-offering-opportunities-dsci-qualys

[33] https://www.cert-in.org.in/

6. **Social engineering attacks: These attacks exploit human psychology to trick individuals into performing actions or disclosing confidential information that could benefit the attacker. For example, phishing, pharming, whaling, etc.**
7. **DDoS attacks: Distributed denial of service (DDoS) is an attack in which attackers gain control of a multitude of computers or devices and employ them in a synchronized assault against the targeted system. DDoS attacks are commonly utilized in conjunction with other cyber threats, often to divert attention and create confusion while executing more covert attacks to steal data or cause further harm.**
8. **Advanced persistent threats: If an individual or group gains unauthorized access to a network and manages to stay hidden for a long period of time, they may attempt to steal sensitive data without being detected by the organization's security team. Such threats are usually carried out by skilled attackers and require significant resources, making them more likely to target nation-states or large corporations.**
9. **Password attacks: An individual's password information can be obtained by a hacker through various methods, such as 'sniffing' the network connection, using social engineering techniques, guessing, or gaining access to a password database.**
10. **Data breach: A data breach occurs when an unauthorized individual views, copies, transmits, steals, or utilizes sensitive or confidential data without permission.**

Cyber threats are motivated by factors beyond financial gain and can stem from revenge, personal gratification, activism, anti-establishment sentiments, and a desire to demonstrate technical prowess. The individuals or groups behind these attacks may range from insiders or small activist groups to organized criminal networks or foreign entities. Prevention of cyberattacks requires a targeted approach, as different types of attacks present unique challenges and require a variety of prevention strategies.

<u>Impact of security breaches on organizations:</u>

1. **Financial loss: A security breach like the theft of financial details or corporate information can lead to significant monetary losses for a company. In a report released by IBM, it was stated that data breaches cost Indian businesses an average of Rs 17.6 crore in 2022.[34] As part of responding to a breach, companies also bear the expenses associated with repairing the affected systems, networks, and devices.**
2. **Reputational damage: If a cyberattack occurs, it may harm the business's reputation and diminish the trust customers have in the company. As a result, the business may lose customers, experience a decrease in sales, and suffer financial losses. Such damages may also affect the company's suppliers, partners, investors, and other third parties involved with the business.**
3. **Legal consequences: In order to comply with data protection and privacy laws, it is necessary to ensure that all personal data related to the business remains secure. If such data is intentionally or unintentionally compromised due to the absence of adequate security measures, the organization can face regulatory sanctions and fines.**

<u>Preparedness to combat cyber threats:</u>

As companies face newer, more sophisticated, and pervasive threats, IT

[34] https://in.newsroom.ibm.com/IBM-Report-Cost-of-Data-Breach-2022?utm_medium=OSocial&utm_source=Twitter&utm_content=RSRW-W&utm_id=CoDBReport22-ISA&social_post=7317964722&linkId=174920190

security departments must realize that the response and fortification against cyber threats need to be an ever evolving process. Understanding security risks within the context of the business is essential, and implementing appropriate controls for infrastructure security is critical. Moreover, educating employees about cybersecurity risks is crucial to mitigate the risks posed by them.

Focusing on network security:

The two fundamental aspects of network security include detection and response. This means that any effective network security strategy should involve swift identification and response to security incidents and threats, as well as implementing measures to mitigate the impact of security incidents and minimize damage. Some critical technologies used in the context of network security are Network Detection and Response (NDR), Extended Detection and Response (XDR), Security Orchestration, Automation, and Response (SOAR) and Security information and Event Management (SIEM).

Mr. Praveen Jaiswal
Co-Chair—FICCI Homeland Security
Co-founder, Vehere

ACCIDENTS



YEAR-ON-YEAR RANKING: In India, industrial accidents happen all too frequently. According to data from the National Disaster Management Authority (NDMA), 130 serious chemical mishaps have been reported in the past ten years, resulting in 259 fatalities and 563 major injuries. Given the data, respondents have voted accidents as the third most prevalent risk for the year 2022. The lives of people working in factories and travelling by land, air, or water can be affected by accidents that happen both within and outside of business premises, such as fires, chemical or gas leaks, explosions, machine accidents, road wrecks, lightning, heat strokes, and landslides.

TRAFFIC ACCIDENTS: Traffic accidents can significantly impact businesses, especially those that rely on transportation. Accidents can result in injury, damage to vehicles or property, and disruptions to business operations. Accidents lead to delayed delivery and reduced productivity for businesses that rely on goods transportation. To mitigate the impact of traffic accidents, businesses can implement safety protocols for employees who drive, such as training on safe driving practices, regular maintenance of vehicles, and enforcing policies on distracted driving.

FORCES OF NATURE – LIGHTNING, HEAT STROKE, LANDSLIDE: Natural disasters like lightning, heatstroke, and landslides can significantly impact businesses. These events can lead to physical damage, power outages, and disruptions to operations. Businesses need contingency plans to address such events, including evacuation plans, backup power supplies, and insurance coverage. Additionally, businesses can take proactive measures such as building lightning protection systems, installing heat-stress monitoring systems, and monitoring weather forecasts to prepare for potential natural disasters.

FACTORY & MACHINE ACCIDENTS: Factory or machine accidents can result in serious injury or death to employees and significant business costs. These accidents can lead to loss of productivity, workers' compensation claims, legal action, and reputational damage. To prevent factory or machine accidents, businesses must provide comprehensive training to employees, perform regular maintenance and inspections of machinery, and implement safety protocols such as wearing personal protective equipment.

CROWD MISMANAGEMENT: Crowd mismanagement refers to the inadequate management of large groups of people in public places such as stadiums, concert venues, or shopping centres. Poor crowd management can result in accidents, stampedes, and injuries to employees or customers. These incidents can cause reputational damage, legal action, and financial loss to the business. Businesses need to have trained staff to manage crowds, implement effective crowd control measures such as using barriers and signs, and regularly review and update their crowd management protocols to ensure the safety of their customers and employees.

INCIDENT MAPPING: The most recent accident happened on January 6, 2022, at the Industrial Development Corporation in Surat as a result of the improper disposal of hazardous chemical waste into a drain. Six workers sleeping nearby and absorbing the toxic vapours perished, while 20 more were hospitalized.[35] Such incidents still occur 37 years after the Bhopal gas tragedy and affect small, medium, and large businesses in the public and commercial sectors, as well as multinational corporations.

The untimely death of a key executive due to a road accident can have a significant impact on a business. The sudden loss of an important leader, like in the case of Cyrus Mistry, can create operational and financial challenges for the organization. The absence of a key decision-maker can disrupt the leadership and decision-making processes, leading to uncertainty and instability. Additionally, the loss of critical knowledge, expertise, and experience can be difficult to replace, potentially causing a long-term impact on the organization. Furthermore, road accidents can also lead to reputational damage, especially if the accident was caused by negligence on the part of the company. This can result in negative media coverage, public scrutiny, and damage to the brand image, which can have long-lasting effects on the organization's relationships with

[35] https://indianexpress.com/article/cities/ahmedabad/6-die-of-toxic-gas-from-tanker-dumping-chemical-waste-7710482/#:~:text=Six%20persons%20suffocated%20to%20death%20and%2023%20others,Development%20Corporation%20%28GIDC%29%20area%20of%20Surat%20Thursday%20morning.

customers, partners, and stakeholders. It can also result in legal and financial liabilities for the organization, leading to financial losses.

With comparison to 2020, in 2021 there were more unintentional deaths (per lakh of the population). In 2021, deaths due to natural causes such as cyclones, tsunamis, landslides, lightning, and torrential rain have increased, while deaths due to avalanche, exposure to cold, tornadoes, floods, and heat stroke have decreased. Deaths due to other causes such as traffic accidents, falls, factory/machine accidents, mines or quarry disasters, and poisoning have increased, while deaths due to air crashes, drowning, electrocution, accidental explosion, and firearms have decreased. There has been a significant increase in deaths due to traffic accident as 173,860 died in 2021, compared to 146,354 deaths in 2020.[36]

IMPACT AND COMBAT: 3 Workers Die Every Day in Indian Factories as per the government data.[37] The labor and safety breaches in the Mundka factory, as revealed by the Working People's Coalition (WPC), pose a significant risk to businesses. Operating without proper licensing from the fire department indicates a lack of adherence to safety regulations and increases the likelihood of accidents and incidents that could harm employees, damage property, and disrupt business operations. The negligence and forgery that enabled the factory to operate without a license demonstrate a disregard for legal and ethical standards that could result in legal action, fines, and damage to the company's reputation.[38]

In addition to the human toll, road crashes lacerate countries' economies by claiming millions of economically productive young lives. As reported by a World Bank Study, road crashes are estimated to cost the Indian economy between 3 to 5 percent of GDP a year.[39]

The high number of road accident deaths in India, with an average of 18 people killed every hour, highlights the urgent need for the country to address road safety. While the government has set an ambitious target to reduce road accident deaths by 50% by 2024, achieving this goal will require a comprehensive approach that goes beyond just infrastructure improvements and law enforcement. It will also require a shift in attitudes towards road safety among all stakeholders, including drivers, pedestrians, and policymakers.[40]

The Andhra Pradesh government has issued new safety guidelines to prevent accidental leakage of toxic gases and chemicals in factories. These measures have been implemented to ensure that such accidents are prevented in the future, given the recent industrial accidents that have occurred in the state. These new guidelines aim to institutionalize preventive measures, such as regular safety inspections, worker training, and emergency preparedness plans. The government's move highlights the importance of prioritizing safety in industrial operations to prevent any harm to workers, businesses, the environment, and the general public.[41]

The Bureau of Indian Standards (BIS) has recently released guidelines for the transportation of dangerous goods in India. The guidelines aim to establish safety requirements for the transportation of hazardous materials, such as flammable and explosive substances, radioactive materials, and other dangerous goods. The guidelines set out specific procedures and requirements for packaging, labelling, and handling of these materials during transportation to ensure the safety of the workers, public, and the environment. Adhering to these guidelines will help prevent potential accidents and mitigate the risk of hazardous materials causing harm during transportation.[42]

These efforts are crucial to ensure the safety of workers and the public, prevent environmental damage, and ultimately protect businesses from potential liabilities. By adopting these guidelines and prioritizing safety measures, businesses can reduce the risk of accidents, maintain their reputation, and avoid financial losses.

[36] https://www.google.com/url?q=https://ncrb.gov.in/sites/default/files/ADSI-2021/adsi2021_Chapter-1Accidents.pdf&sa=D&source=docs&ust=1678951072436093&usg=AOvVaw0g7WCDww6gHI8sAA46XCht

[37] https://www.indiaspend.com/special-reports/3-workers-die-every-day-in-indian-factories-govt-data-show-850083

[38] https://workingpeoplescharter.in/media_statements/public-release-mundka-fire-fact-finding-report-access-to-minimum-wages/

[39] https://blogs.worldbank.org/endpovertyinsouthasia/how-do-poor-cope-road-crashes-india

[40] https://www.google.com/url?q=https://www.moneycontrol.com/news/business/what-is-india-doing-to-reduce-the-worrying-rate-of-road-accidents-9133301.html&sa=D&source=docs&ust=1678951072545991&usg=AOvVaw0VnGvkswgOVb-8yww8XFYT

[41] https://economictimes.indiatimes.com/news/india/andhra-govt-brings-out-new-safety-guidelines-to-check-industrial-accidents/articleshow/94613969.cms

[42] https://affairscloud.com/current-affairs-9-march-2023/

BUSINESS ESPIONAGE



YEAR-ON-YEAR RANKING: Given the rise in the competitive landscape and opponents always preying on the trade secrets, Business Espionage has been voted at the 4th spot by the surveyors.

RISK THROUGH DOCUMENT WASTE: Risk through document waste refers to the potential risks associated with the improper disposal of confidential business documents. These documents may contain sensitive customer data, financial information, and trade secrets. Businesses must implement secure document destruction protocols, such as shredding or incineration, to prevent unauthorized individuals from accessing such information. Failure to implement such protocols can result in losing confidential information, reputational damage, and legal action.

HACKING / INSIDER THREAT: Hacking and insider threats are growing business concerns as technology advances. These threats can lead to data breaches, identity theft, and loss of intellectual property. Businesses need to implement robust cybersecurity measures, such as firewalls, encryption, and two-factor authentication, to protect their digital assets from these threats. Additionally, employees need to be trained on safe online practices and the importance of protecting confidential information.

VENDOR BRIBING: Vendor bribing refers to offering bribes or kickbacks to vendors to gain an unfair advantage in business transactions. This can include offering incentives to vendors to win contracts or gain access to confidential information. Businesses need clear policies to prevent vendor bribing and ensure that all business transactions are conducted ethically and transparently. Failure to prevent vendor bribing can result in legal action, reputational damage, and financial loss.

EMPLOYEE POACHING: Employee poaching refers to recruiting employees from rival or competitor business firm. This can lead to losing skilled employees, impacting a business's productivity and profitability. To prevent employee poaching, businesses must create a positive work environment, offer competitive compensation packages, and provide professional growth and development opportunities. Additionally, businesses can implement non-compete agreements to prevent employees from leaving to work for competitors.

INCIDENT MAPPING: Business espionage through document waste, insider threat, vendor bribing, and employee poaching can cause significant harm to businesses. These sub-risks can result in the leakage of sensitive information, loss of trade secrets, reputational damage, financial losses, and legal liabilities. Therefore, businesses must take preventive measures such as conducting regular risk assessments, implementing robust security policies and protocols, providing employee training, and monitoring the use of confidential information.

Hackers sponsored by neighbouring countries had targeted India's power infrastructure in Ladakh, according to information released by the American cybersecurity company Recorded Future on April 6, 2022. The persistent attack on India's power grids may have been part of cyber espionage strategy of certain countries to learn more about India's vital infrastructure or to prepare to harm it. It is yet unknown what technical data the hackers obtained through this intrusion. Offensive cyber operations against India have been continuing for more than a decade. It targets the power infrastructure and cyber-espionage effort that fits this larger pattern. Some global business entities having operations in India have revealed unabated campaign sponsored from outside India to steal trade and other sensitive data.

IMPACT AND COMBAT: While India has not proved such an attractive target for commercial cyber espionage agenda run by a neighbouring nation, things may change. Two Indian vaccine manufacturers, Bharat Biotech and the Serum Institute of India (SII), had their information technology systems targeted by a foreign state-sponsored hacker organization.[43] The most important component of India's national immunization program and vaccine diplomacy has been the use of vaccines produced by these firms. Hackers' targeting of SII is significant given that Covishield by Oxford-AstraZeneca is used in 183 countries. In contrast, Sinopharm, the vaccine for SII, is used in just about half that many (used in 90 countries). The Indian Prime Minister's description of India as the "pharmacy

[43] https://www.reuters.com/article/health-coronavirus-india-china-idUSKCN2AT21O

of the world" succinctly summarises its comparative advantage over its adjacent economies. Hackers may be attempting to close that gap by attacking vaccine manufacturers to acquire data that has economic value.[44]

India is taking steps to strengthen its online security and is also launching offensive cyber operations to counter cyber espionage activities from its neighboring country. However, it is suggested that India needs to do more. One important step for the Indian government is to provide technical evidence linking these cyber-attacks to foreign state-sponsored hackers, which the national security establishment has been reluctant to do so far. This is in contrast to the technical community in India and other countries who have already established such links. Thus, business espionage can impact businesses by compromising their confidential information, trade secrets, and intellectual property leading to reputation and financial loss. To combat espionage, businesses should implement security measures such as proper document disposal, employee training and monitoring, background checks on vendors & partners, and secure data storage & communication systems.

THREATS TO WOMEN SAFETY



YEAR-ON-YEAR RANKING: Academics assert that the contribution made by women is crucial to a society's economic and political transformation. Women's work, both official and informal, can change society from an independent society to an active participant in the national economy. However, with the rise in participation, the cases of violence and discrimination against women have also been scaling up. This year, Threats to Women's safety has dramatically jumped to the fifth position from the last position.

EVE-TEASING: Eve-teasing can lead to a hostile work environment for female employees, negatively impacting their productivity and mental health. Companies must create a safe and inclusive work environment for all employees, conduct regular training and awareness programs on sexual harassment, and implement strict policies to address such incidents.

ABDUCTION: Abduction is a serious crime that can significantly impact businesses, particularly those that employ individuals who may be at risk of being abducted. This can include employees working in remote locations or those who travel frequently. To protect female employees from abduction, businesses must conduct risk assessments to identify vulnerable employees, provide security training, and implement protocols to ensure their safety while traveling.

SEXUAL FAVORS AT WORKPLACE: Sexual favors refer to offering or accepting sexual favors in exchange for professional benefits such as promotions, raises, or career advancement. This can lead to a hostile work environment, decrease employee morale, and negatively impact business performance. Companies must create a safe and inclusive work environment, establish clear policies on workplace harassment, and enforce strict penalties for violations.

SEXUAL ASSAULT: Sexual assault is a serious crime that can significantly impact businesses. Such incidents can occur within the workplace or during work-related events, leading to legal action, reputational damage, and loss of productivity. Businesses need to create a safe and inclusive work environment, conduct training and awareness programs on sexual harassment and assault, and implement clear policies on how to report incidents of sexual assault. Businesses must take all reports of sexual assault seriously and investigate them promptly and thoroughly.

Incident Mapping: The increase in sexual harassment cases reported by top companies in India highlights the need for safer workplace environments. Despite the Sexual Harassment of Women at Workplace Act being passed in 2013, sexual harassment cases continue to pose a threat to women's safety and dignity. A data analysis compiled by Complykaro.com shows that the total number of sexual harassment complaints in workplaces increased by 27% in the financial year ending March 2022 compared to the previous year. While the work-from-home arrangement initially reduced sexual harassment complaints, they have started to rise again as return to

[44] https://www.orfonline.org/expert-speak/expanding-chinese-cyber-espionage-threat-against-india/

office phase has started.[45]

Recent statistics reveal that women entrepreneurs make up an important portion of India's business landscape, with 8 million women owning 10% of all formal businesses and 14% of all entrepreneurs. Women-owned firms are a crucial part of the MSME sector, accounting for roughly 20.37% and employing around 23.3% of the labor force. Women entrepreneurs own between 13.5 and 15.7 million enterprises, employing between 22 to 27 million people and are considered the cornerstone of India's economy. Increasing career options for women and reducing the stress associated with working two shifts per week can be achieved by adopting the 3Rs approach, which recognises, reduces and redistributes unpaid care work provided by women. It is imperative that all areas of legislation embrace this approach to enable women entrepreneurs to continue contribute significantly to India's economy.[46]

Despite India's vast population, the country's formal workforce has barely seen one in five women participate in the workforce over the last two decades. The number of women in the labor force has declined significantly, highlighting a pressing need to address gender disparity in employment. According to Colliers, approximately 52% of women in India are employable, yet the number of women who are actually employed remains alarmingly low. This issue is particularly concerning given that women are a crucial driving force in the Indian economy. The lack of women's participation in the formal workforce not only has economic implications but also has broader societal implications, such as reduced opportunities for women in the business world. Efforts must be made to address these issues and increase women's participation in the workforce to achieve a more equitable and prosperous society.[47]

IMPACT AND COMBAT: Women in India who strive to become financially independent and work in different sectors, including government, private and non-profit, often face harassment from bosses, co-workers and third parties. According to the National Crime Record Bureau's 2021 report, 418 cases of workplace harassment were recorded.[48] Workplace harassment is not limited to sexual harassment, but it includes various types that affect an employee's mental health, causing humiliation and mental torture, affecting their working capacity and a dropout from work. Women in different professions, including police officers, factory workers, and corporate executives, often face harassment due to fear and the power dynamic between the perpetrator and victim. Victims of harassment are often afraid to report such incidents for fear of retaliation from their superiors, fear of confrontation, fear of being fired, and fear that it would affect their career prospects. Mental health issues caused by the harassment are often overlooked in many organisations, but it is crucial to promote awareness among employers and employees about mental health disorders. A recent study by the WHO estimated that depression and anxiety disorders cost the global economy approximately USD 1 trillion each year in lost productivity.[49]

Women who are subjected to harassment in the workplace can suffer from a range of mental and physical health issues, such as depression, PTSD, and high blood pressure. Despite the government's efforts to combat harassment, many women still do not feel comfortable reporting such incidents due to fear of retaliation and the stigma surrounding mental health issues. The 'Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013' has been effective in providing a sense of security to female employees, but more needs to be done to raise awareness about the impact of harassment and encourage reporting. It is important to create a workplace culture that fosters safety and support for victims, and to take necessary measures to ensure that perpetrators are held accountable.[50]

[45] https://www.forbesindia.com/article/take-one-big-story-of-the-day/rise-in-sexual-harassment-cases-in-indias-top-companies-shows-dichotomy/80721/1

[46] https://news.abplive.com/business/international-womens-day-contribution-of-women-entrepreneurs-towards-india-s-economic-growth-how-they-are-shaping-the-future-1586785

[47] http://www.businesstoday.in/latest/corporate/story/office-design-location-accessibility-play-a-huge-role-in-creating-women-friendly-workplaces-colliers-372669-2023-03-08

[48] https://www.clearias.com/ncrb-report-2021/

[49] https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(20)30432-0/fulltext

[50] https://www.indiablooms.com/news-details/M/87433/workplace-harassment-the-truth-about-women-s-labor-force-participation-decline.html

NATURAL HAZARDS



YEAR-ON-YEAR-RANKING: Earlier, Natural Hazards ranked as the top risk but now as the aftermath of pandemic is declining, it is positioned at the 6th place. Natural hazards can have significant impact on businesses, particularly in terms of physical damage to assets, disruptions to supply chains, and decreased productivity. Floods, for example, can lead to lost revenue and increased costs due to damage to physical assets and disruptions to logistics and transportation. A pandemic can cause decline in productivity due to employee absences, and disruptions to supply chains eventually leading to inflation. Droughts and famines can lead to decreased agricultural productivity and food shortages, impacting businesses that rely on these resources. Earthquakes can cause physical damage to buildings and equipments, leading to lost revenue and increased costs. In addition to the direct impacts, natural hazards can also cause disruptions to local infrastructure and utilities that businesses rely on.

INCIDENT MAPPING: India is facing a notable risk from climate change, with the country being ranked as the third-most vulnerable country globally, according to a recent report by XDI. The report also revealed that nine of India's states are among the top 50 most at-risk regions. Despite this high vulnerability, India's capacity to protect itself from potential economic damage caused by natural disasters remains low. For instance, at a recent UN Security Council meeting, Mumbai was declared a 'high-risk' area due to rising sea levels. Furthermore, the 2022 Bengaluru floods resulted in economic losses of Rs 10,000 crore to Karnataka, yet the insurance pay out was less than Rs 400 crore. Experts estimate that the insurance industry could have covered risks up to Rs 5,000-7,000 crore, which could have significantly reduced overall losses. Similarly, during the Chennai floods of 2019-20, the insurance industry paid only Rs 1,200 crore despite the overall economic loss amounting to about Rs 16,000 crore. These examples highlight the need to strengthen its resilience against natural disasters and improve its insurance coverage to mitigate economic losses caused by climate change.[51]

IMPACT & COMBAT: The southwest monsoon approaches India every year in June, and Kerala is typically the first state to be affected. Residents in Kerala, South India, consistently experience difficulties as a consequence of floods brought on by the region's constant monsoon rains. Due to a cyclonic circulation over Rayalaseema, a north-south trough, and a shear zone across south peninsular India, Kerala saw significant downpours in August 2022. When the flood situation worsened, the water level in several major rivers rose, particularly in the districts, forcing the inhabitants to take shelter at relief camps.[52]

One of the most important things businesses can do is to ensure that their insurance policies cover the risks of natural disasters. Many policies now exclude coverage for events such as floods or landslides, so it is essential to check that your policy provides adequate protection.

Despite being ranked among the top five best-performing countries in climate change, India experienced an unprecedented number of climate-related events in 2022, according to a report by the Centre for Science and Environment. These events occurred on 241 out of 273 days between January and October 2022, causing consequential damage to life and property. The report reveals that these events cost over 2,755 lives, affected 1.8 million hectares of crop area, destroyed over 416,667 houses, and killed close to 70,000 livestock. This highlights the new normal of more extreme events and disaster risks that we are living in.[53]

Recognizing the severity of climate change, the Reserve Bank of India (RBI) released a discussion paper on climate change and sustainable finance in July 2022. The paper emphasizes that climate change is a real and significant economic risk and without mitigation, the entire financial sector is vulnerable. Therefore, the RBI recommends that banks start reflecting climate risk on their balance sheets and lending propositions, which will have clear implications for the Indian industry and its credit in the future. Climate inaction has created a financial time bomb, and it is crucial to prioritize measures to address this issue to safeguard both the environment and the economy.[54]

[51] https://fintech.global/2023/03/09/weathering-the-storm-with-parametric-insurance/

[52] https://www.nipfp.org.in/media/medialibrary/2022/04/WP_383_2022.pdf

[53] https://weather.com/en-IN/india/climate-change/news/2022-11-02-india-saw-a-climate-change-natural-disaster-every-day-in-2022

[54] https://www.google.com/url?q=https://www.forbesindia.com/article/isbinsight/financial-time-bomb-the-risks-of-climate-inaction-to-the-global-economy/83163/1&sa=D&source=docs&ust=1678951072453932&usg=AOvVaw3V93yRp2ulMa_FCT1FYDTs

Another way to reduce the risk of natural hazards is to invest in mitigation measures such as flood defences or earthquake-resistant buildings. These measures can help reduce the damage caused by natural disasters and make it easier and cheaper to recover from an event.

Finally, it is important to have a good business continuity plan in case of a natural disaster.

Localizing Disaster Risk Reduction

As we were adjusting to the new normal after COVID pandemic, Indian subcontinent experienced extreme weather events for 314 days (almost one event every day) in 2022, sparing no state. Many of my fellow business leaders have experienced disruptions during COVID and thereafter due to sudden extreme weather conditions and witnessed how status quo can get altered overnight throwing our plans into disarray while leaving a trial of damage on our balance sheets and growth strategies.

As per the report published by the World Meteorological Organization and the UN Economic and Social Commission for Asia and the Pacific (ESCAP), India suffered huge economic losses from floods and storms in 2021 as climate change made these events more frequent. India suffered a total loss of $3.2 billion from flooding. The country faced heavy rains and flash floods during the monsoon season between June and September 2021. These events resulted in about 1,300 casualties and damaged crops and properties.

Over the last two decades, a paradigm shift has taken place from disaster relief to a holistic approach with emphasis on disaster prevention, mitigation and preparedness. The Government of India has strengthened institutional arrangements for Disaster Risk Reduction (DRR) with the enactment of the Disaster Management Act, 2005 and by setting up an apex authority i.e. National Disaster Management Authority under the Chairmanship of Hon'ble Prime Minister.

The Government of India has recognized the need to evolve a consultative process of decision-making in disaster management with the active involvement of Central and State Governments and all concerned stakeholders in the field of disaster management. These steps have helped in reducing the number of casualties over the decades. As per a paper published by IMD scientists, the decade from 1970-1980 recorded over 20,000 mortalities due to cyclones. Mortality rate associated with tropical cyclones decreased by almost 88 per cent in the decade 2010-2019 in comparison to the earlier decade 2000-2009 despite the significant increase severe tropical cyclones over Bay of Bengal. Better disaster preparedness based on geographical analysis and use of GIS in building cyclone shelters and evacuation planning played major role.

With change being constant, ongoing physical and digital infrastructure transformations are altering the business landscape rapidly and will continue to do so. Adoption of technologies, improved connectivity, growth of e-commerce, and focus on sustainability and social responsibility are reinventing the supply chain upstream as well as downstream. Business ecosystems are more connected and integrated than ever and are also somewhat becoming more resilient to disasters.

Redefining Disaster Contextualization

Historically, DRR has always been perceived to be a government function. By and large the studies and forecasts carried out by the agencies are at macro level, which do not necessarily intersect with our business operations. Added to the limitations with which agencies operate, high stakes involved for individual businesses make it imperative to contextualize the disaster risk at a micro-level taking local business conditions into account.

With natural disasters continuing to be beyond the realm of human control, business leaders are left with only option of "Preparing - Responding -

Recovering". Localized DRR approach embedded in our growth strategies can help us to stay ahead and battle against odds. This is an imminent need no business leader can postpone any longer.

Localize, Reduce and Prevent Geospatially

A geographical understanding becomes starting point for the businesses to localize their DRR. Leveraging powerful capabilities of geospatial technologies, businesses can visualize and assess their risks with localized insights and strategize how to see, think, and act during disruptions. As a powerful tool, Geospatial technology supports DRR efforts to mitigate business disruptions. By applying spatial analysis, businesses can qualify, quantify, and visualize the hazard probability, exposure, and vulnerability of operations at a micro level. Coupled with site vulnerability analysis, GIS helps identify alternative scenarios to support risk mitigation.

Prepare Better

Localized disaster preparedness helps businesses to contextualize the business operations, understand where an extreme weather event or disruption will occur and how the operations can best prepare to protect, and take anticipatory action to manage disruptions. GIS provides tools and systems to monitor known hazards and forecast events, create location-specific early warning systems and alerting platforms, and identify vulnerable sites and alternates for business continuity.

Respond in Time

With real-time location intelligence tools, crisis teams can quickly make sense of volatile situations and take steps to prioritize activities including impact assessment, needs analysis, prioritization, field mission management, and progress monitoring. Informative spatial dashboards aid to quickly analyze impact, and assess needs, helping businesses to take informed decisions in time. Spatial analysis tools integrated with mobile and field applications help driving response and coordination plans dynamically.

Recover Faster

Rebuilding the networks and stabilizing the ecosystem is a vital step in disaster recovery. GIS based disaster recovery solutions enable businesses to express priority requirements, design reconstruction plans, provide a transparent account on recovery progress, and build better resilience for the future. Using advanced spatial analysis and dashboards GIS enables efficient communication and collaboration that is transparent and inclusive at all points during recovery, while exuding stakeholder confidence.

In Closing

With increasing frequency and suddenness of weather-related extreme events and disruptions businesses are at increased risk of getting trapped into situations that are detrimental and could derail their growth stories. Nature's fury often renders humans helpless. But going by trend of damages these disasters are inflicting, we all realize that risk reduction is something which we can do and is in our hands.

Localizing disaster risk reduction by "Preparing strategically, responding rapidly and recovering methodically" is the instinct we business leaders

need to proactively cultivate. By going for geo-enabled DRR framework, our businesses will be better placed to anticipate risk, prepare, and deal with the eventualities, while staying on track with our dreams, vision, and stakeholders' interests.

Mr. Agendra Kumar
Chair – FICCI Committee on Geospatial Technologies and
Managing Director, Esri India

FIRE



YEAR-ON-YEAR RANKING: Office and commercial building fires frequently have terrible and far-reaching effects. Even though property damage might seem to be the most obvious consequence of a fire, there are numerous other losses, such as the impact a fire has on an employee's mental and physical health, that make a business's ability to recover exceedingly challenging. This year Fire has been ranked at the 7th position by the respondents.

Electrical short circuits and chemical fires can cause physical damage to buildings and assets, leading to lost revenue and increased costs. Fires in buildings, public transport, and gas cylinder or stove bursts also pose severe threats, leading to physical damage to infrastructure & assets and also disrupting transportation & logistics, which can have a cascading impact on businesses. Beyond the direct impact of the incidents, fires also attract increased regulatory scrutiny and decreased consumer confidence, causing further damage to businesses, particularly if the incident harms individuals. Addressing these sub risks requires businesses to develop appropriate risk management strategies to mitigate the impact of these incidents, ensuring business continuity and safeguarding their assets and employees.

INCIDENT MAPPING: According to data accessed by PTI, Delhi's fire service received 16,518 fire-related calls in 2022, out of which 722 were non-fatal, while 82 resulted in fatalities. These alarming statistics highlight the importance of fire safety measures in the city. Businesses, in particular, can suffer a significant impact due to fire incidents. A fire can result in severe damage to property leading to high financial losses. Additionally, businesses can face legal and regulatory consequences if they fail to adhere to fire safety regulations.[55]

As per the records maintained by the Brihanmumbai Municipal Corporation (BMC), almost 70% of fire incidents in Mumbai are caused due to electric short circuits. This highlights the importance of ensuring proper electrical safety measures in factories and industrial buildings across the city. Electrical short circuits can result in devastating consequences, including property damage, injury, and even loss of life. To prevent such incidents, it is crucial to undertake regular maintenance of electrical systems, install appropriate safety equipment such as circuit breakers, and avoid overloading electrical outlets.[56]

In the Mundka neighborhood of Delhi, India, on May 13, 2022, a fire broke out on the first level of a four-story office and commercial structure. At least 50 people were saved, and 142 were reported dead and 40 others were hurt. A short circuit is thought to have ignited the fire. The fire department had not given the structure approval, and the building lacked fire extinguishers. The fire was reported by the Delhi police as a criminal conspiracy and culpable homicide.[57]

IMPACT & COMBAT: Frequent risk assessments and ongoing modifications to the working environments and practises may also help to avoid dire outcomes.

Nonetheless, nobody is ever completely safe from unforeseen circumstances. Any company should thus have a catastrophe recovery plan that outlines how it will respond to the effects of fire damage. Such a strategy should specify not only the actions the management should take in the event of a commercial fire, but also the contacts of the specialists they should call, in particular a fire damage restoration firm, to avoid difficult decisions or time lost. Even though no service can completely eliminate the negative impacts of fire damage to businesses, prompt professional assistance from a fire damage restoration firm can frequently play a critical role in reducing the amount of downtime and the associated losses. Therefore, it is crucial for businesses to prioritize fire safety measures by conducting regular audits, installing appropriate fire safety equipment such as extinguishers, alarms, and sprinklers, and training employees on fire safety protocols. Ensuring fire safety not only protects businesses from financial loss but also saves precious lives.

[55] https://www.google.com/url?q=https://timesofindia.indiatimes.com/city/delhi/more-than-16500-fire-related-incidents-claimed-82-lives-in-2022-delhi-fire-service/articleshow/97006720.cms&sa=D&source=docs&ust=1678951072570268&usg=AOvVaw0cMpOSCFJXpYxCdmG-WiStu

[56] https://indianexpress.com/article/cities/mumbai/nearly-70-of-fire-incidents-due-to-electric-short-circuits-8281725/

[57] https://indianexpress.com/article/cities/mumbai/nearly-70-of-fire-incidents-due-to-electric-short-circuits-8281725/

CRIME



YEAR-ON-YEAR RANKING: The negative effects of Crime are present in every country in the world. Nonetheless, some nations experience more negative effects than others. India is a developing country of 1.3 billion people with soaring crime rates. In past years various crimes, especially crimes against women have increased. The respondents have voted “Crime” as the 8th major threat to the businesses in 2022.
Property crimes, including burglary, theft, and vandalism, can result in significant damage to physical assets and infrastructure, leading to lost revenue and increased costs. Violent crimes such as murder and kidnapping can cause serious harm to employees and customers, leading to decreased morale and consumer confidence. Offences against public tranquillity, such as riots and civil unrest, can cause physical damage to buildings and infrastructure, impacting businesses that operate in high-risk areas. Drug abuse can also negatively impact businesses, leading to security risks and decreased productivity among employees.

The decrease in the number of cognizable crimes registered in 2021 is a positive development for India’s criminal justice system. With a decline of 7.6% in the number of cases reported in 2021 compared to 2020, it indicates a reduction in criminal activity. Moreover, the fall in the crime rate from 487.8 in 2020 to 445.9 in 2021 indicates that fewer crimes were committed per lakh population, indicating a more secure environment for people. However, it is concerning that the number of SLL offences increased by 3.7% compared to the previous year, while IPC cases fell by 13.9%. The percentage proportion of IPC cases was 60.1%, while SLL cases accounted for 39.9% of the total cognizable crimes in 2021.[58]

INCIDENT MAPPING: According to a report, around 67% of Indian organizations that faced fraud identified, external attacks or a combination of internal and external sources as the most disruptive incidents. This is an increase from the 56% reported in 2020.[59]

Misconduct, or bad actors working together and taking advantage of the uncertainty and volatility brought on by the Epidemic, was the main problem organizations had to deal with. At 90%, conduct risk posed the greatest hazard and was related to company personnel, vendors, agents, and clients.

IMPACT AND COMBAT: Researchers have mixed views on economic growth and crime, and most of the studies are based on Crime as one of the factors influencing the country’s economic growth and not the other way around. However, the studies have two varying theories regarding the impact of economic growth on crime rates. One is that a bad economy might force a person to commit crimes to make ends meet, and another one is that a thriving economy may increase crime rates. A wealthy neighbourhood might experience more property crime and robberies because of the availability of items of more excellent value.

As a result of the disruption brought on by Covid-19, 95% of them experienced new sorts of fraud. According to a survey released more than 50% of Indian enterprises encountered an economic crime in the previous 24 months, and 95% experienced new sorts of fraud due to the disruption brought on by Covid-19.
According to a Study 2022: India Insights, business prevention efforts reduced these instances from 69% in 2020 to 52% in the previous two years.[60]

In the previous 24 months, fraud affected up to 60% of Indian businesses, with global annual revenues of over $1 billion. 37% of businesses with global annual revenues under $100 million reported fraud during this time. 47% of businesses reported customer fraud involving mortgages, credit cards, claims, and checks. Second, with 45% of businesses reporting similar instances, was cybercrime. 34% of Indian businesses that experienced financial crime reported KYC failure.[61]

[58] https://ncrb.gov.in/sites/default/files/CII-2021/CII_2021Volume 1.pdf

[59] https://www.pwc.in/consulting/forensics/pwcs-global-economic-crime-and-fraud-survey-2022.html

[60] https://www.ndtv.com/business/pricewaterhousecoopers-over-95-organisations-in-india-faced-new-fraud-incidents-in-past-2-years-says-survey-3522552

[61] https://www.business-standard.com/article/companies/over-50-indian-firms-experienced-economic-crime-in-2-years-survey-122111501212_1.html

POLITICAL & GOVERNANCE INSTABILITY



YEAR-ON-YEAR RANKING: Political & Governance Instability drops to the seventh rank from last year's fifth position in the India Risk Survey 2022. The presence of a stable political and governance structure is often seen as essential for achieving planned economic growth in emerging economies like those in Asia. Political instability, on the other hand, can lead to uncertainties and risks for businesses, including changes in policies & regulations, potential civil unrest and violence, and increased corruption. The idea that economic growth is the best approach to ensure political stability may be widely accepted. According to this view, political instability is mostly caused by the disparity between ambitions and realities or between resources and demands. The best course of action is to close this gap as quickly as possible through economic development.

Political and governance instability can also impact businesses, particularly in terms of regulatory uncertainty, disruptions to supply chains, and decreased security. State fragility can lead to increased security risks and regulatory uncertainty, particularly in regions where businesses operate. Changes in policies, regulations, and laws can lead to increased costs and decreased revenue for businesses, particularly those that are impacted by these changes. Instability at the local government level can cause disruptions in services and utilities that businesses rely on, including transportation and logistics. International conflicts can cause disruptions to supply chains, increased costs, and decreased revenue, impacting businesses that rely on these relationships. In addition to the direct impacts, political & governance instability can also cause decreased consumer confidence, further impacting businesses.

> **"Business is fraught with risk, more so in the aerospace and defence domain. With the changing geo-political scenario, this risk has increased. With India's rapid emergence as a leading player in international trade in defence and aerospace, the risks have also multiplied. It is in this background that the IRS assumes greater significance for the Indian industry. I am sure the Indian companies will benefit immensely from this survey."**
>
> — **Mr Neeraj Gupta**
> Chair – FICCI Homeland Security Committee
> Managing Director, MKU Ltd.

India has made remarkable progress in enhancing its Ease of Doing Business ranking, as per the World Bank's latest report. The country has shown a significant jump of 79 positions, from the 142nd spot in 2014 to 63rd in 2019. In the World Bank's Doing Business 2020 assessment, India secured the 63rd position among the 190 countries analyzed. In 2014, the Indian government launched an aspiring program of regulatory reforms with the objective of simplifying business procedures and regulations in the country. These persistent efforts have resulted in India being recognized as one of the top 10 improvers for the third consecutive year, with a notable improvement of 67 positions in just three years. These achievements are expected to make India an even more attractive destination for foreign investment and businesses looking to operate in the country.[62]

INCIDENT MAPPING: These governance and political leadership indicators measure a country's ability to develop through effective governance. The study further discovered that a one-point increase in the political stability index results in a 1.38% to 1.62% increase in GDP both in the short and long term. Similarly, Radu (2015) found a significant positive relationship between Romanian political stability and economic growth. A strong rule

[62] https://www.makeinindia.com/eodb#:~:text=India%20jumps%2079%20positions%20from,of%20Doing%20Business%20Ranking%20 2020%27.&text=To%20further%20enhance%20the%20ease,legal%20provisions%20have%20been%20decriminalized

of law is linked to low levels of political instability and significantly impacts economic growth.[63]

IMPACT AND COMBAT: Although political stability and good governance are important, many other factors can influence economic growth. As a result, they must not be overlooked. While making a quantitative analysis, measuring the impact of political stability and good governance on economic growth without controlling for other variables may be misleading. According to Fayissa and Nsiah (2013), the impact of good governance on economic growth in Sub-Saharan African economies varies depending on socioeconomic levels at the two ends of the income distribution spectrum—low and affluent. Hussain (2014) has a very critical opinion in this regard, stating that political stability resulting from having one party or a coalition of parties in power for a long time may adversely impact long-term economic growth.[64]

The Indian government is moving ahead with its plan to introduce the Digital India Act (DIA), which will replace the outdated IT Act 2000. In its first public consultation, the government engaged with industry and policy stakeholders to gather feedback and suggestions for the new legislation. The DIA is a much-needed update to the existing legal framework, which was crafted at a time when the internet was in its infancy. With the rapid evolution of technology and the proliferation of digital services, the government recognizes the need for a modern, comprehensive legislation that can address emerging challenges and protect the interests of all stakeholders. The government's consultation with industry and policy experts is a step towards creating a robust legal framework that can enable India to fully realize the potential of its digital economy.[65]

India has become one of the most alluring locations, both for investments and for conducting business. India moves up 79 spots in the World Bank's 2020 Ease of Doing Business Ranking, from 142nd in 2014 to 63rd in 2019. The position of India on this metric rose from 184 in 2014 to 27 in 2019.4 This improvement is primarily attributable to a reduction in the number of steps and length of time required to get construction licences in India.

The position of India on this metric rose from 137 in 2014 to 22 in 2019. In India, obtaining an energy connection for a business just requires four procedures and 53 days.

Aside from these noteworthy advancements, India ranks 25th in obtaining credit and 13th in protecting minority investors among the 190 economies.

Governmental changes are required as time and circumstances change, or political stability can take the form of complacency and stagnation, preventing competition. On the other hand, political stability and long-term dominance by a single party or a coalition of parties can also boost economic growth if they change with time, support productive activities and investment projects, minimize investor risk, and increase return on investment.[66]

CORRUPTION, BRIBERY & CORPORATE FRAUDS



YEAR-ON-YEAR RANKING: Corruption lowers resource quality, which lowers investment productivity. "Corruption, Bribery & Corporate Frauds" has maintained its position at the 10th spot in the India Risk Survey 2022. For instance, corruption lowers a nation's human capital through decreasing the number and quality of health and education services. Rent-seeking behaviour also tends to lead to inefficiencies, which encourage resource waste and reduce the effectiveness of public spending. Self-dealing and covert transactions undermine mechanisms like political representation and economic efficiency. Corruption makes it possible for party officials, bureaucrats, and contractors to use funds allocated for elections, health care, education, and poverty assistance as a means of personal gain.

[63] https://link.springer.com/article/10.1007/s40847-022-00199-9

[64] https://econpapers.repec.org/article/jdajournl/vol.47_3ayear_3a2013_3aissue1_3app_3a91-108.htm

[65] https://www.livemint.com/news/government-holds-first-consultation-on-digital-india-act-to-replace-it-act-2000-11678440033837.html

[66] https://link.springer.com/article/10.1007/s40847-022-00199-9

Corruption, bribery, and corporate frauds are striking risks that businesses need to address. These activities can lead to severe financial and reputational harm, negatively impacting the bottom line and eroding public trust. Bribery and kickbacks can create an unfair advantage, allowing unethical businesses to gain market share at the expense of ethical competitors. The use of shell companies and conflicts of interest can cause financial losses and damage to a company's reputation. Furthermore, the theft of business identity can have severe implications, affecting a company's operations, intellectual property, and reputation.

INCIDENT MAPPING: In the past 24 months, 52% of Indian organisations suffered fraud or economic crime, according to a survey. Remarkably, 95% of them reported experiencing new fraud categories, such as misbehaviour risk (67%), legal risk (16%), cybercrime (31%), insider trading (19%), and platform risk (38%). The pandemic has caused a rise in financial institution fraud.[66]

According to the analysis, Covid-19's disruption prompted new fraud instances in 95% of the organisations that had already experienced fraud in India.

IMPACT AND COMBAT: Businesses are finding it difficult to prevent fraud, with over 67% of the organizations polled stating that an external attack or coordination between external and internal parties was the cause of the incident that caused the most disruption. Customers (41%), organized crime (31%), and hackers (49%), respectively, were the most frequent external offenders.[67]

Yet, the impact of fraud and economic crimes on both large and small firms varied. According to the a survey, large organizations are more prone to fall prey to fraud or other forms of cybercrime. 60% of questioned Indian businesses with global yearly revenues above $1 billion reported fraud overall within the previous 24 months.
On the other hand, just 37% of surveyed organizations, with global annual revenues of less than $100 million, encountered fraud over the same period.

In terms of financial losses, around 14% of organisations lost $50 million or more, 28% lost between $1-$50 million, and 50% lost less than $1 million owing to all cases of fraud, corruption or other economic crimes over the last 24 months.

STRIKES, CLOSURE, & UNREST



YEAR-ON-YEAR RANKING: The rank of "Strikes, Closure & Unrest" has dropped to the 11th position as compared to the previous year, which was at the 8th position. Strikes, closures, and other forms of disturbance have an immediate negative impact on a business's revenues and activities. Companies may choose to shut down operations during such disruptive events, but protesters may also target specific companies and damage their property at any scheduled or unplanned gathering.

Strikes, closures, and civil unrest are risks that can have consequential impacts on businesses. Labor strikes can cause supply chain disruptions and decreased productivity, leading to financial losses. Civil unrest, such as protests and demonstrations, can result in property damage and decreased consumer confidence, impacting businesses' revenue streams. Political violence also poses a serious risk to businesses operating in high-risk areas. Regulatory changes can also negatively affect businesses, leading to increased costs and reduced revenue.

INCIDENT MAPPING: Over 50 million people participated in India's two-day nationwide strike in March 2022 a much less number that was anticipated.

Workers at banks, factories, and public transportation systems disrupted services in six states, but the strike had a minor overall impact.

Ten trade unions issued the call for a strike in response to the widespread economic hardship that workers are currently facing due to lost jobs, declining incomes, exorbitant prices for basic necessities like food and fuel, and long-term unemployment—all of which have been made worse by the Covid-19 pandemic.

[67] https://dazeinfo.com/2022/11/16/indian-companies-experienced-fraud-or-economic-crime-following-covid-19-report/

Universal social security coverage, a higher minimum salary, a stop to the sale of state assets, and no more privatization of public sector banks were among the demands voiced by the unions.[68]

IMPACT AND COMBAT: The system's liquidity is controlled by banks, which constitute a pillar of the economy. Banks act as a multiplier of money since they take deposits. While preserving some of the money as reserves, the accepted cash is lent out. Bank strikes halt this routine activity. In addition to potentially harming the viability of the financial system over the long term, this might cause a credit crunch in the economy over the short term. Strikes may result in lower productivity, which indicates lower short-term profitability. The clearing of import and export bills is also accelerated. The effectiveness of the nation on a worldwide scale is impacted by this.

TERRORISM & INSURGENCY



YEAR-ON-YEAR RANKING: India, a developing nation, is confronting several difficulties in contrast to many other wealthy nations. In recent years incidences of terrorist operations have dropped significantly due to economic sanctions on terrorist outfits and India's stand against terrorism. Terrorism & Insurgency has consequently scored the lowest position in India Risk Survey 2022.

Terrorism & insurgency pose significant threats to businesses, ranging from physical damage to assets, disruptions to supply chains, and decreased consumer confidence. Incidents such as active shooter attacks, suicide bombings, and insider threats can result in significant loss of life and damage to physical assets, severely impacting businesses operating in high-risk areas. Explosive devices and CBRNE attacks can also cause significant physical damage to buildings and infrastructure, leading to lost revenue and increased costs. Narco-terrorism further compounds the situation by adding security risks and regulatory uncertainties, adversely affecting businesses. The disruption of transportation and logistics caused by these incidents further exacerbates the negative impact on businesses.

INCIDENT MAPPING: In Kashmir, there were total 93 successful encounters in 2022, which resulted in the neutralization of 172 militants, including 42 international terrorists.[69]

IMPACT AND COMBAT: The effects of terrorism on the Indian economy, according to economists, are diverse, intricate and precise. The terrorist attacks have significant short-term and long-term effects on the Indian economy.

The Quad members - US, India, Japan, and Australia - have criticized activities promoting terrorism and pledged to cooperate with Indo-Pacific partners to address the issue. The countries also expressed their commitment to supporting Pacific Island nations in areas such as climate change, resilient infrastructure, and maritime security, to strengthen the Indian Ocean Rim Association. India's leadership in finalizing the IORA and holding the G20 Presidency has been greatly appreciated, and cooperation among the Quad Group countries is seen as a step towards building a new apparatus to manage terrorism.[70]

In addition, recently India and Germany highlighted active cooperation to fight terrorism.[71]

The induction of various gadgets and equipment like, bomb/bulletproof armored vehicles is a significant step towards ensuring successful anti-terror operations. Such vehicles provide much-needed protection to the security personnel during counter-terrorism operations and help in minimizing collateral damage. These operations can

[68] https://www.nytimes.com/2022/03/28/world/asia/india-modi-general-strike.html

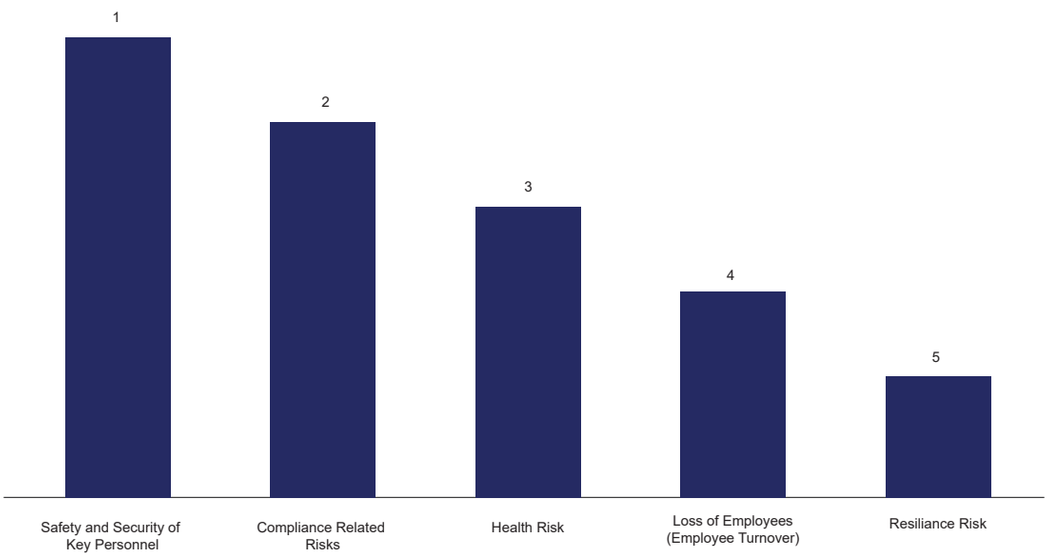
[69] https://www.ndtv.com/india-news/172-terrorists-killed-in-over-90-operations-in-kashmir-in-2022-senior-cop-3653181

[70] https://www.google.com/url?q=https://www.dailypioneer.com/2023/columnists/how-to-combat-global-terrorism.html&sa=D&source=docs&ust=1678951072557217&usg=AOvVaw0BknvhGDeFl6L5_3KRQQCP

[71] https://www.google.com/url?q=https://www.devdiscourse.com/article/agency-wire/2362515-theres-active-cooperation-between-india-germany-in-fight-against-terrorism-separatism-pm-modi-after-talks-with-german-chan&sa=D&source=docs&ust=1678951072557268&usg=AOvVaw3qW8bZAmvxGMEp4tzJF6O0

also help create a more secure environment for businesses to operate in the region. The threat of terrorism can have a negative impact on businesses, leading to reduced investment and hindering economic growth. By taking steps to counter terrorism, the government can help create a more conducive environment for businesses to thrive, which can have a positive impact on the overall economy.[72]

Emerging Risks



As the world becomes increasingly connected, businesses face new risks and challenges. The top significant emerging risk is the **Safety and Security of Key Personnel**. As more businesses operate globally, their key personnel are often located in different parts of the world. This creates new challenges in terms of keeping them safe and secure. Any organization's major asset is its human capital but maintaining that asset's safety and security is difficult due to a variety of internal and external challenges. It has become more difficult in today's dynamic risk environment to provide key personnel with a secure work environment, even outside the office, while on domestic and international business travel. Several factors contribute to the safety and security of key personnel as there always is a risk of civil unrest. These include the political and security environment in which they are located, their security arrangements, and the security of their work premises.

The **Compliance-Related Risk** is emerging as the second biggest risk for businesses. The regulatory environment constantly changes, and businesses must keep up with the latest compliance requirements. The regulations that apply to firms tend to change rapidly which makes it hard for everyone to keep a tab on the rules. That's why it is essential to keep the policies and procedures updated, inform the workforce of the most recent laws, and ensure

[72] https://www.google.com/url?q=https://www.wionews.com/india-news/crpf-introduces-critical-situation-response-vehicle-to-fight-terrorists-in-kashmir-region-567657&sa=D&source=docs&ust=1678951072557318&usg=AOvVaw1sEpW9cOobLnHWiwWcb9vP

that the business is in full compliance at all times. The significance of recruiting the right talent in defending the firm from compliance-related risks has been emphasized by this dynamic situation. Furthermore, businesses must ensure their employees are properly trained on compliance-related issues. Failure to do so can result in significant fines and penalties. Thus, businesses need to have a robust compliance program in place.

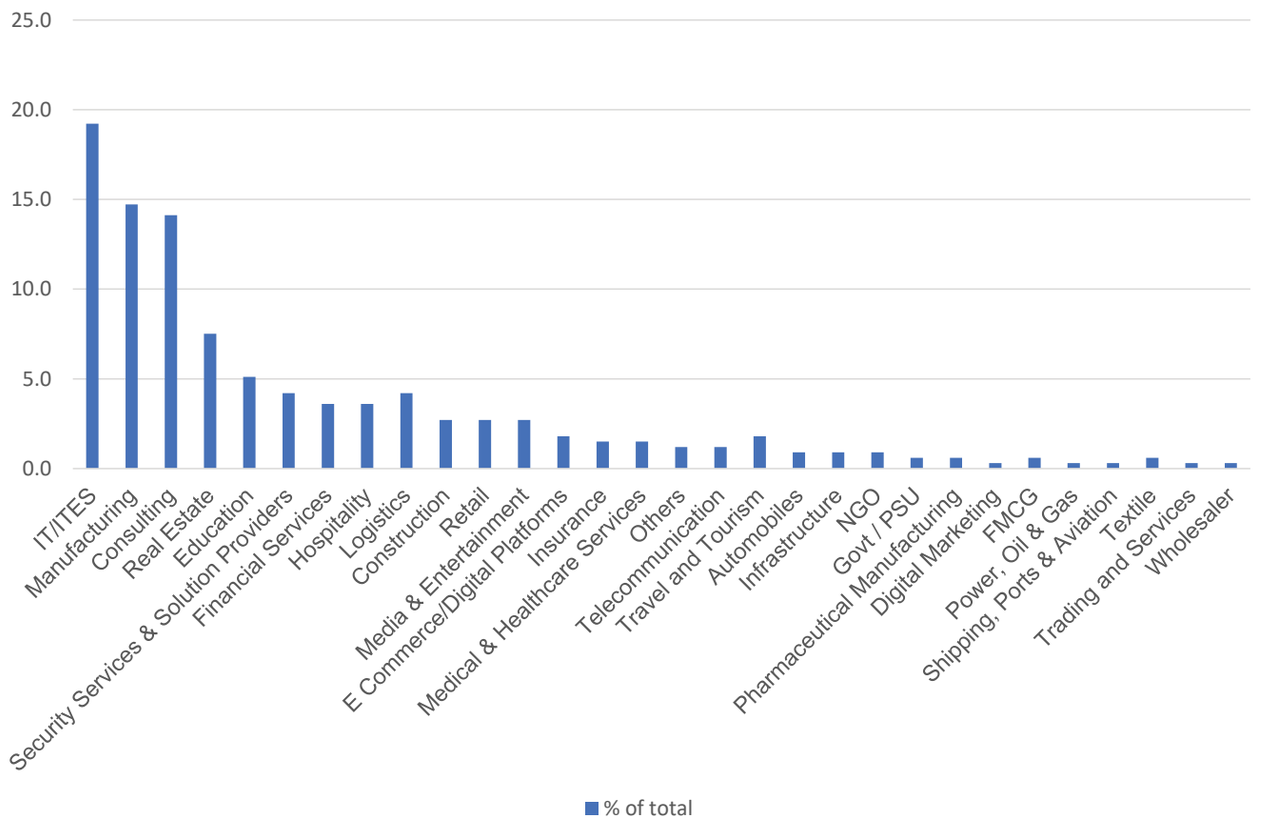
Health Risk has been placed in the third position in this fast-paced world, where people struggle to cope with their mental and physical health and find work-life balance. The pandemic has had a profound impact on our mental health. The stress and anxiety of living through a global pandemic has taken a toll on our mental health. After working in isolation for two years, both employees and employers are finding it difficult to re-join the offices again. People have become more socially anxious and are unable to perform up to their potential strength.

In recent years, businesses have become increasingly aware of the risks of **Loss of Employees (Employee Turnover)** and ranked them in the fourth position. This is particularly true in today's economy, where the war for talent is more intense than ever. As the workforce slowly begins to return to the office, organizations are facing mass resignations and deliberate layoffs. For some, the remote working environment simply doesn't suit their needs or lifestyle. For others, the pandemic has been a wake-up call, leading them to reassess their priorities and decide that it's time to move on. The practise of switching employment, which was previously observed within a sector, has now been extended across several disciplines and domains. There have been numerous occasions where a senior employee joining a competitor resulted in significant business loss. The risk of moonlighting has increased as more people work from remote areas. This can significantly impact a company's bottom line and even lead to the failure of the business.

Resilience Risk is a critical concept for understanding and addressing the challenges of sustainable development in an era of growing risk and uncertainty. A risk-resilient organization can both foresee future challenges and capitalize on opportunities to successfully balance risk and reward. In an ever-changing business landscape, resilience is an increasingly important quality for businesses. Hence the respondents have voted the resilience risk in the fifth spot. The ability to weather storms, adapt to new challenges and maintain a positive outlook despite setbacks is essential for long-term success.

Methodology & Respondents

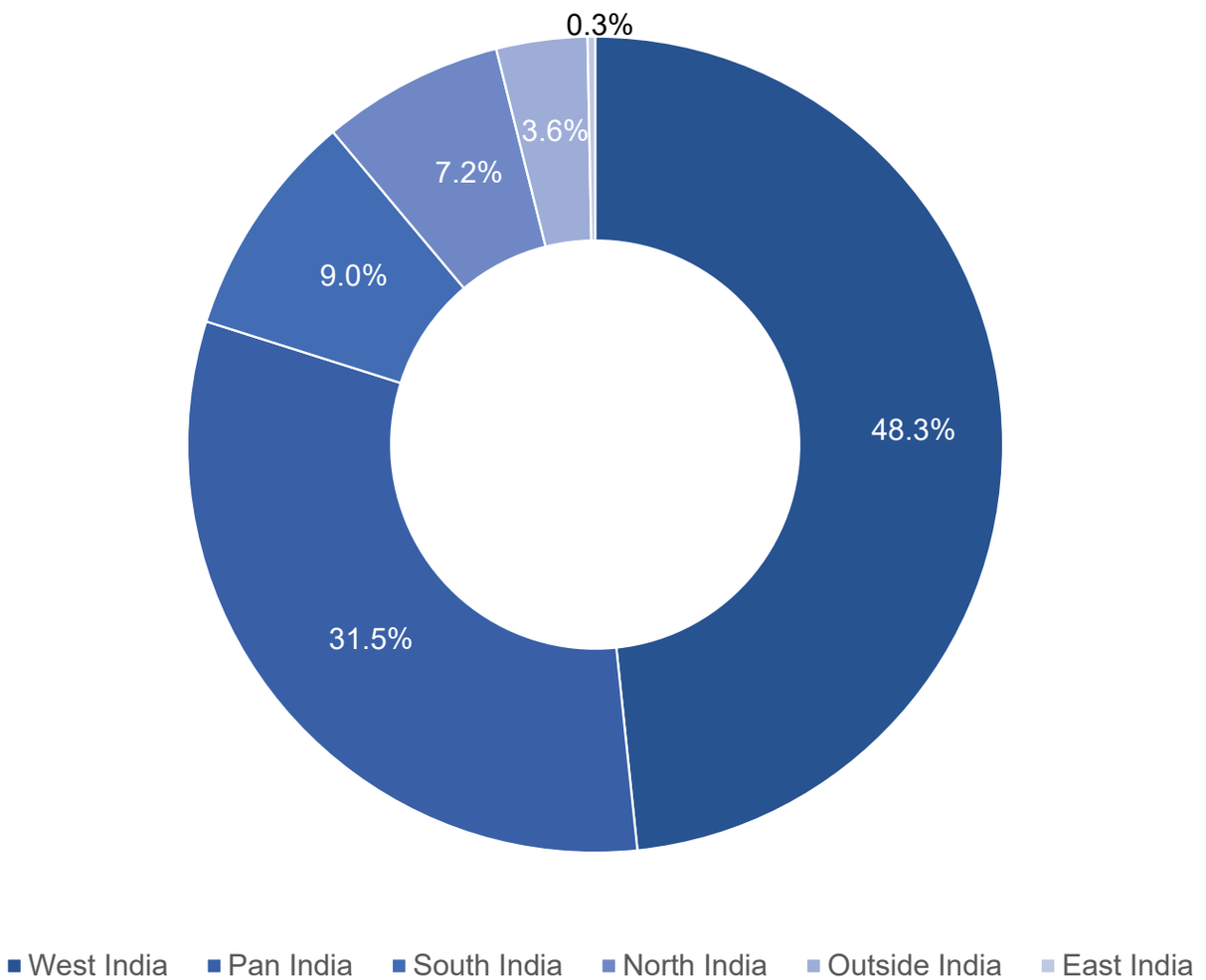
INDUSTORY WISE CONTRIBUTION



The objective of IRS 2022 is to identify critical risks and rank them according to their increasing importance for Indian enterprises and geographical areas. An international and domestic risk survey was used as part of the technique. The responses included workers at all levels of management, from middle to upper. Each risk's trend observations have been included with the graphic presentation of all results. The most prominent and prevailing risk is given the number 1 rank and the least prominent one is placed at number 12 rank Also, respondents had to specify which threat fell under each risk category occurring frequently.

Geographical Contribution

RESPONDENTS OPERATING FROM



Way Forward

Risk is an integral part of any business. Every financial choice and economic activity involve some level of risk. Businesses may safeguard and increase their equity by comprehending and controlling risk.

In today's rapidly evolving digital landscape, intellectual property theft and information & cyber insecurity present critical threats to Indian businesses. The proliferation of digital platforms and the increasing reliance on advanced technologies have created a fertile ground for cyber threats and intellectual property infringements. These risks have far-reaching implications, including financial losses, reputational damages, and compromised intellectual property, leading to a significant competitive disadvantage.

To effectively address these risks, Indian businesses must adopt a proactive approach to a comprehensive risk mitigation strategy covering both cybersecurity and intellectual property protection along with the physical security of assets. This requires implementing comprehensive data security protocols, regularly assessing the organization's vulnerabilities, investing in advanced software and hardware systems, and providing comprehensive employee training and awareness programs. In addition, businesses should engage with risk advisors, cybersecurity experts and intellectual property advisors to devise strategies that safeguard their proprietary assets.

By prioritizing on cybersecurity and intellectual property rights along with physical security, Indian businesses can effectively mitigate these risks and value add in their businesses by reflecting a good risk governance approach with a competitive edge to win the customer and investor trust and help them compete globally.

ABOUT PINKERTON

Pinkerton is a global comprehensive risk and security management leader focused on delivering specialized risk advisory, investigations, protection solutions, and embedded SMEs. With over 170 years of legacy, Pinkerton has built unparallel institutional knowledge, while having sight into future risk businesses are facing.

We bring a total risk perspective, knowledge-based design, and end-to-end delivery in everything we do. With our three-pronged approach, we assess the risk factors you are facing today, design an effective solution that fits your unique needs, and can deliver tactical services to assist you with execution — in an ad hoc to prolonged capacity.

As a trusted partner, you can rely on our family of thousands of employees and connected partners across 100+ countries to support your risk management and security needs.

We never sleep.

PINKERTON®

WE NEVER SLEEP

WWW.PINKERTON.COM



ABOUT FICCI

Established in 1927, FICCI is the largest and oldest apex business organisation in India. Its history is closely interwoven with India's struggle for independence, its industrialisation, and its emergence as one of the most rapidly growing global economies.

A non-government, not-for-profit organisation, FICCI is the voice of India's business and industry. From influencing policy to encouraging debate, engaging with policy makers and civil society, FICCI articulates the views and concerns of industry. It serves its members from the Indian private and public corporate sectors and multinational companies, drawing its strength from diverse regional chambers of commerce and industry across states, reaching out to over 2,50,000 companies.

FICCI provides a platform for networking and consensus building within and across sectors and is the first port of call for Indian industry, policy makers and the international business community.

NOTES

NOTES

NOTES

NOTES





ROHIT KARNATAK

Vice President | India
APAC & EMEA – Global Screening
C: +91 981-855-5924
Email : Rohit.Karnatak@pinkerton.com

MANDEEP KAUR

Marketing & Sales Manager | India
Email : Mandeep.Kaur@pinkerton.com

Pinkerton
Plot # 17, Sector 44
Gurgaon - 122002 (Haryana) India
Tel. : +91 124 4645400
www.pinkerton.com

SHANTANU KRISHNA

Managing Director | India
Email : shantanu.krishna@pinkerton.com

Office No. 505, 5th Floor, Eastern
Court, Sion - Trombay Rd,
Chembur, Mumbai - 400071
(Maharashtra) India

SUMEET GUPTA

Assistant Secretary General
FICCI
Federation House, Tansen Marg,
New Delhi - 110 001

Tel. : +91 11 2373 8760-70
Fax : +91 11 23765333
Email : sumeet.gupta@ficci.com

GAURAV GAUR

Joint Director
FICCI
Federation House, Tansen Marg,
New Delhi - 110 001

Mob : +91 9873 111 690
Fax : +91 11 23765333
Email : gaurav.gaur@ficci.com

www.ficci.in

PINKERTON
GLOBAL HEADQUARTERS
101 N. MAIN STREET
ANN ARBOR, MICHIGAN
48104, UNITED STATES

WE NEVER SLEEP
WWW.PINKERTON.COM