MARSH | RIMS the risk management society

EXCELLENCE IN RISK MANAGEMENT | NOVEMBER 2018

State of Risk Management in India

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES | Asia Pacific Risk Center

EXCELLENCE IN RISK MANAGEMENT | NOVEMBER 2018

State of Risk Management in India

CONTENTS

Introduction

In an increasingly complex, volatile, and interconnected world, risk management has assumed greater significance. Technological advancements have revolutionized business practices, but are also posing new challenges to manage and contain risk. More companies are recognizing the need and importance of implementing a comprehensive risk management framework which can improve their ability to anticipate, categorize, and transform risks into sustainable competitive advantages.

The corporate risk management landscape is evolving in India as well. With growing acceptance from senior management, the risk function is moving closer to the boardroom. Risk management teams are now expected to take on a greater role not only in terms of leading risk governance and compliance, but also in actively influencing strategic growth decisions by addressing new and emerging risks. Risk management in India is at a turning point where risk managers are constantly looking at avenues to expand their knowledge base, hone their skillsets, and gain access to best practices, tools, and technology.

At this unique juncture, Marsh and RIMS, the risk management society™ have collaborated to produce this joint study which sheds light on the maturity of risk management functions in corporate India. This study addresses the following areas of interest:

- What are the top risks Indian corporates face?
- How mature is risk management in organizations?
- What are the key areas of risk management that require improvement?
- What are the risks in adopting emerging technologies?
- Key recommendations for risk executives

Marsh and RIMS have a long history of collaborating to advance knowledge and best practices in risk management, with the "Excellence in Risk Management" series being published annually in many geographies. We are excited to launch the inaugural report at RIMS' first risk management forum in India.

Marsh India has been present in the Indian market for over 15 years, and has been providing risk and insurance advisory to 4000+ corporates. RIMS is the preeminent organization dedicated to educating, engaging and advocating for the global risk community. RIMS is in the process of registering itself in India and launching an India Chapter by 2019 to expand its presence in India and Asia. It seeks to create a knowledge space for Indian risk management professionals through a growing and increasingly localized resource base of whitepapers, reports, tools, certifications, and a global community of over 10,000 plus risk professionals.

In India, RIMS and Marsh aim to provide an ongoing platform for established and aspiring risk professionals in the country to advance the discussion on risk management. Together we will share best practices and produce reports at regular intervals through annual forums, discussion events, and closed-door summits.

We hope this report stimulates discussions in your organization about opportunities to adopt risk management practices that support strategic initiatives. We encourage you to reach out to us with any questions or comments.

Sanjay Kedia

SANJAY KEDIA
Country Head and CEO
Marsh India

ROBERT CARTWRIGHT, JR.
2018 President
RIMS, the risk management society™

Mary Roth

MARY ROTH
Chief Executive Officer
RIMS, the risk management society™

Top Risk Concerns in India

In 2018, the world witnessed several tumultuous developments, resulting in a wide array of technological, environmental, geopolitical, and economic problems.[1] From cyberattacks in various parts of the world to major hurricanes and floods in Asia-Pacific in 2017 and 2018, and from the unexpected developments around North Korea to the US-China trade war in 2018, several key global risks have crystallized.

India is not exempt from the increasingly diverse and rapidly evolving risk landscape, and corporate India needs to set up enterprise risk management practices in a way that is agile and responsive to this environment. In the inaugural survey for the Marsh RIMS Excellence in Risk Management State of Operations in India, survey respondents were asked to choose critical risks that are impacting their organizations now, and risks that will be impacting them in one to three years, and in more than three years. The survey aims to gauge organizational thinking about emerging risks over different time horizons.

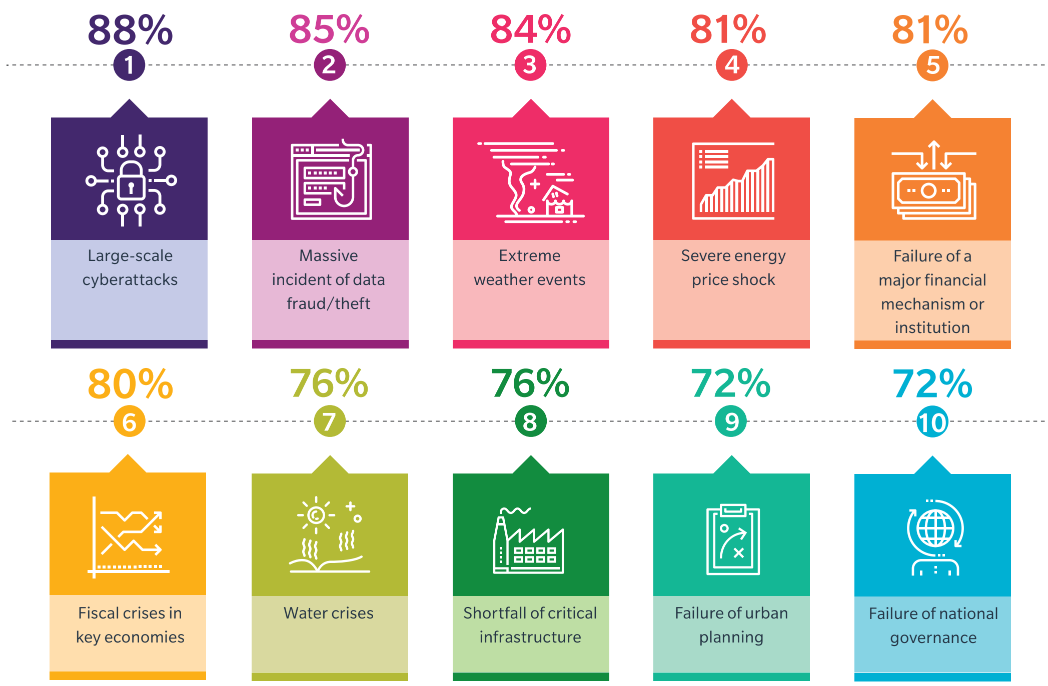
Large-scale Cyberattacks and Data Fraud Top the List

The top 10 critical risks are highlighted below *(Figure 1)*.

Large scale cyberattacks (88 percent) and massive incidents of data fraud or theft (85 percent) lead as top risks for survey respondents – India's growing dependency on data and digitization efforts has increased the risk of cyberattacks. Just this May, the Indian Computer Emergency Response Team (CERT-In) found that over 22,000 Indian websites, including 114 government portals, were hacked between April 2017 and January 2018.[2] Furthermore, as reported by The Tribune,[3] high profile data theft incidents such as the breach on Aadhaar, India's national database, have left unfavorable impressions on risk professionals in India that not just businesses but even the government is inadequately prepared to handle cyberattacks and data breaches.

FIGURE 1

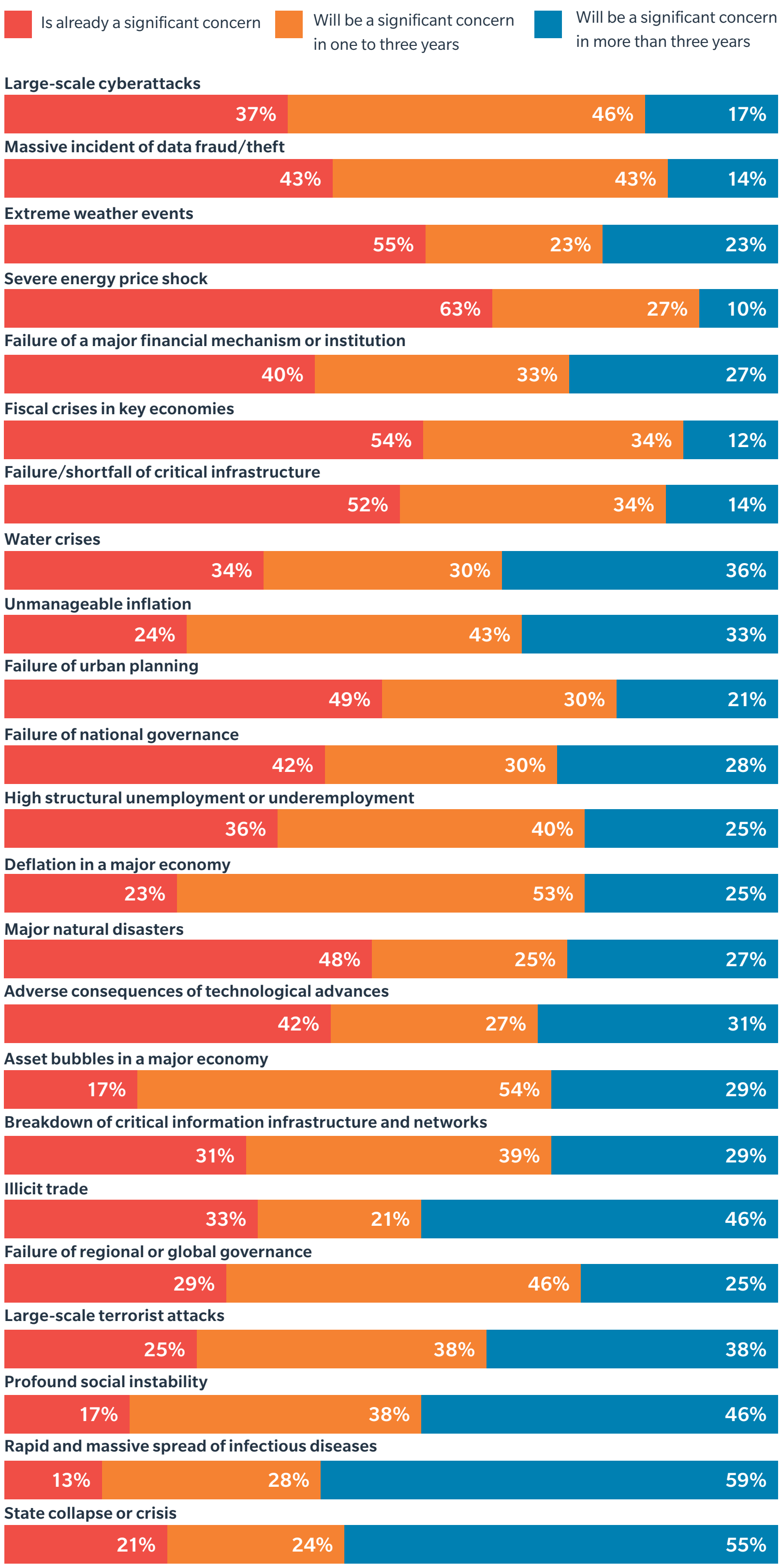
From which of the following areas will the next critical risks for your organization emerge?



Three broad categories were identified for these risks (*Figure 2*).

FIGURE 2

Please state the time frame in which you think the next critical risks will impact your organization



"Large scale cyberattacks (88 percent) and massive incidents of data fraud or theft (85 percent) lead as top risks for survey respondents"

"India's growing dependency on data and digitization efforts have increased the risk of cyberattacks"

Contemporary Risks

These are present day risks that are already of significant concern to organizations. The top emerging risks that respondents cited were:

- **Severe energy price shocks**: The recently released Energy Trilemma Index[4] by the World Economic Forum (WEF) and Oliver Wyman put India's energy security far below that of developed nations. India's energy security is facing challenges on three fronts simultaneously. First, India is heavily reliant on oil for its industries, importing 82 percent of its oil needs in 2016-2017.[5] Second, its yearly consumption has more than doubled over the past two decades. And lastly, its domestic production has been declining since 2010, based on data from the Ministry of Petroleum & Natural Gas. The recent sanctions by the US on Iran and the decision by the Organization of the Petroleum Exporting Countries to not increase output have pushed up oil prices.[6] A continuing upward trend of Brent crude oil prices[7] will not only adversely impact businesses, but also the country's economy as a whole. Indeed, this is such a pressing issue that at the recent India Energy Forum in October 2018, India's Prime Minister Narendra Modi raised the issue of high crude oil prices to oil producers, saying that it is causing "consumer pain".[6]

- **Extreme weather events**: The implications of climate change are particularly severe for India. The Global Climate Risk Index – 2018, released by Germanwatch, ranked India as the sixth most affected country in the world in 2016. India lost the most number of human lives (2,119) compared to other countries and suffered over $21 billion in property losses as a result of climate change.[8] One of the largest flood in India happened in August 2018 in Kerala, due to unusually high rainfall during the monsoon season, resulting in a large number of human fatalities and significant property damage. According to a report by Lloyd's,[9] India has one of the largest insurance gaps globally for natural catastrophes with a penetration rate of less than 1 percent, highlighting the vulnerability businesses face when extreme weather events occur. In the case of the recent flood in Kerala, the state's Chief Minister pegged the initial damage at over INR195 billion ($2.7 billion).[10] Kerala's agriculture sector, one of the largest contributors of India's Gross Value Added (GVA) at 15.4 percent,[11] saw losses for tea plantations alone amounting to around INR9 billion ($122 million).[10] This event highlights how extreme weather events can cause catastrophic damage to businesses in India.

India has one of the largest insurance gaps globally for natural catastrophes with a penetration rate of less than 1 percent

SOURCE: LLOYD'S'

Imminent Risks

Shifting to a longer-term outlook (one to three years from now) by survey respondents, the top two risks were economic and political instability, followed by technology risks.

- **Asset bubbles in a major economy**: Asset bubbles shoulder the blame for some of the most devastating recessions the world has faced. Over the past years, the longest bull run in the equity markets has experienced recent shake ups in the markets. Many experts believe that a sustained bear market might crystalize in the near future.

- **Failure of regional or global governance**: The ongoing trade war initiated by the US has shaken up global trade and supply chains. The Trump administration's America First foreign policy has seen tariffs being imposed on Indian steel and aluminum, which resulted in exports of Indian steel items to the US falling by 42 percent.[13] India's longstanding territorial disputes with Pakistan and China over Kashmir also pose a significant political threat to the region. The continued tensions between India and Pakistan often result in armed attacks and clashes at the Line of Control, the de facto border between the two countries in the region. This has severely affected the tourism industry in Kashmir where many areas have been cut off from tourists due to unrest.

- **Large-scale cyberattacks**: Although the possibility of large-scale cyberattacks was the overall top risk for 88 percent of respondents, responses were split across two risk horizons. A little over a third (37 percent) respondents believe cyberattacks are highly prevalent now, and 46 percent are of the view that it is an imminent critical risk. This can be attributed to different risk maturity levels of respondents' organizations, as well as their experiences with such attacks either directly or by witnessing attacks on industries at large. According to leading security surveys, India ranked third on the list of countries with the highest number of cyber threat detections, and second in terms of targeted attacks in 2017.[14] There is also a very strong correlation between cyberattacks and data breaches. A study by Gemalto's Breach Level Index highlighted that a majority of data breaches came from malicious outsiders (56 percent), with accidental loss (34 percent) as the next source.[15]

- **Massive incidence of data fraud/ thefts**: A study by the Ponemon Institute and IBM Security found that India had the highest average number of breached records at 33,000 in 2017 as compared to the global average of 24,000. The study also found that the average cost of a data breach in India has been on the rise, growing by nearly 8 percent year-on-year in 2017 to INR11.9 crore ($1.68 million).[16] In January this year, The Tribune[3] reported that the Government of India's Aadhaar fell prey to a severe data breach. For just 500 rupees ($7), an anonymous service allowed anyone access to all of the nearly 1.2 billion Indian citizens' personal information. An additional 300 rupees ($4) yielded access to software through which anyone could print an ID card corresponding to any Aadhaar number. This illustrates the vulnerability and lack of preparedness organizations in India face towards data fraud incidents.

Risks on the Horizon

These are complex, uncertain and often broad threats that can have unexpected adverse effects on organizations. Specifically pointing at the time at which these trends will become critical is difficult, but that does not mean they go ignored.

- **State collapse or crisis and profound social instability**: More than half (55 percent) of the respondents chose state collapse as the top risk in the future (more than three years from now). This is in parallel with a similar risk – profound social instability – at 46 percent. India frequently experiences domestic unrest stemming from a variety of sources – these include political grievances, labor-related strikes, farmer grievances and entrenched socio-economic inequality emanating from the caste system. In January 2018, for example, Mumbai came to a standstill as protestors from the Dalit community came out in the thousands to protest violence by right wing groups against members of their community.[17] This forced many businesses across the city to close their doors, resulting in costly business disruptions.

- **Rapid and massive spread of infectious diseases**: India already faces challenges from a range of infectious diseases like dengue and chikungunya. The number of chikungunya cases is believed to have increased by 30 percent over the past three years.[18] Additionally, exacerbating the spread of diseases in India is a burgeoning population, rapid urbanization, and increasing human mobility. Threats of superbugs and multi-resistant antibiotic infections are also a major public health threat in India where broad-spectrum drugs such as carbapenems, which are the antibiotics of last resort, have seen increased usage.[19] The rapid and massive spread of infectious diseases poses a problem for businesses due to the potential health care costs, higher employee absenteeism, lower productivity, and severe epidemics that can cause business interruptions or even industry shutdowns.

- **Water crisis**: This was the only risk that saw an almost equal number of respondents choosing it across three risk horizons, highlighting this as a perennial problem for India. India is home to 16 percent of the world's population but only possesses 4 percent of its fresh water.[20] To make matters worse, water scarcity in India is expected to worsen as the overall population is expected to increase to 1.6 billion by the year 2050. Water quality is also marred by industrial pollution and human waste. Both these issues pose health threats to employees of businesses. Furthermore, water dependent businesses are also affected – for example, 90 percent of India's thermal power generation depends on fresh water for cooling. Fourteen of India's 20 largest thermal utilities experienced at least one shutdown due to water shortages between 2013 to 2016, costing the companies $1.4 billion.[21]

Fourteen of India's 20 largest thermal utilities experienced at least one shutdown due to water shortages between 2013 to 2016, costing the companies $1.4 billion

SOURCE: WORLD RESOURCES INSTITUTE

Risk Forecasting Expected to Become Even More Difficult – Interconnectivity of Risks a Major Challenge

The risk landscape is evolving rapidly. The interconnected dynamics of geopolitics, technological advances, global economic integration, social instability, and climate change mean that the manifestation of one risk is increasingly likely to influence others. For example, when a known risk, such as critical infrastructure failure, meets with emerging risks such as cyberattacks or data breaches, the outcomes become harder to predict. New combinations of risks may exacerbate the magnitude and surface area of impacts on organizations, especially those that are unprepared for the growing convergence of longstanding and emerging risks. This means there is a growing need to anticipate emerging risks, and the ability to predict potential outcomes when risks intersect.

Furthermore, identifying risks beforehand allows risk management teams to be more efficient and accurate in allocating their resources, and also allows senior leaders to build a stronger case to their boards for resources to address such risks.

Success in risk management, therefore, often comes to organizations that develop a multi-dimensional approach to identifying and managing complex risks. Key requirements for a robust risk identification process include both analytical and operational characteristics *(Figure 3)*. Organizations that do so are able to predict emerging risks and understand that they may interact with existing risks in unpredictable ways.

FIGURE 3

Key requirements for a robust risk identification process

SOURCE: MARSH & MCLENNAN COMPANIES' GLOBAL RISK CENTER

Analytical Characteristics

COMPREHENSIVENESS

- Established and emerging risks
- On and off balance sheet
- Measurable and "hard to model"

GRANULARITY

- Casual events/drivers as well as risk types
- Includes relationship between risks and business activities

MATERIALITY ASSESSEMENT FRAMEWORK

- Consistent framework acros all risk types
- Typically based on likelihood and severity of occurrence

Operational Characteristics

ENGAGEMENT OF SENIOR MANAGEMENT AND BUSINESSES

- Improves "top-down" risk identification
- Sets the tone for rest of organization
- Ensure better linking of risks to business activities
- Enables more timely identification of emerging risks

DOCUMENTATION

- Consistent risk assessment template to document risks, their drivers and materiality
- Centralization of disparate information on different risk types

FREQUENCY

- Annual review to ensure outputs remain current
- Updates as necessary to reflect changes in business

Forty-seven percent of survey respondents find forecasting of critical risks either "more difficult" or "significantly more difficult" today compared to three years ago (*Figure 4*). This finding was less pronounced in a similar survey in the US in 2016,[22] where only 32 percent of US respondents thought that it was more difficult.

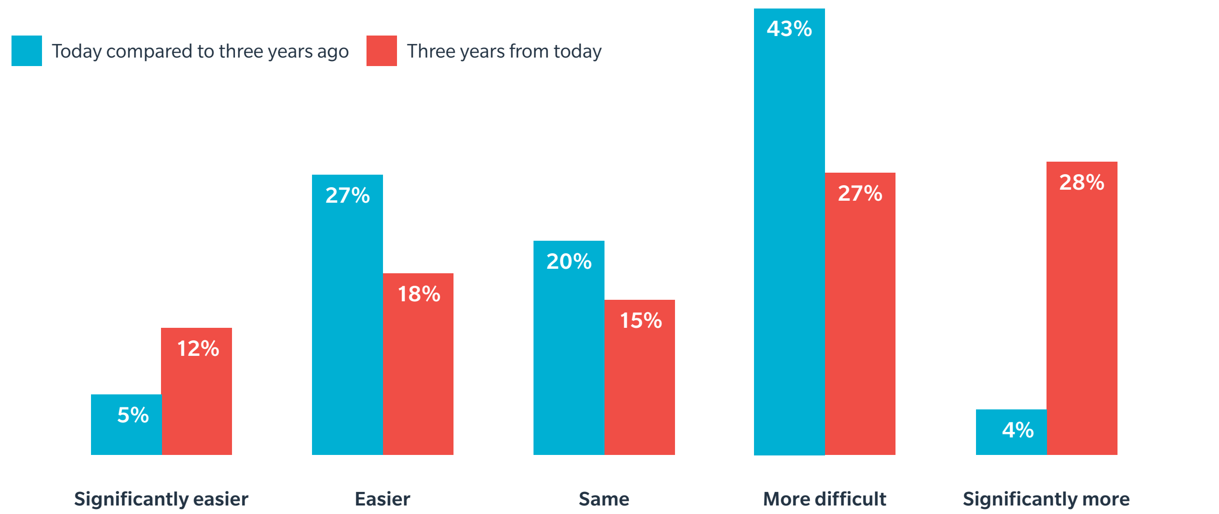
More notably, 28 percent of Indian respondents believe they will face significantly more difficulties in forecasting critical risks in the future compared to only 8 percent of US respondents.

Although India faces an inherently different set of problems compared to the US, the expectations expressed in the survey highlight the different levels of maturity in forecasting risks.

"New combinations of risk may exacerbate the magnitude and surface area of impacts on organizations, especially organizations that are unprepared for the growing convergence of longstanding and emerging risks"

FIGURE 4

How much easier/more difficult is it to forecast critical risks to your business today compared to three years ago, and what are your expectations three years from today?



State of Implementation in India

In this study, we seek to understand the level of maturity of comprehensive risk management in India by looking at how well Indian corporates identify, assess, communicate, and handle risk.

While best efforts have been made to cover a broad range of survey respondents by industry, job position, and company size, this is but a snapshot of a larger and multi-dimensional challenge. To address any potential biases, we have supplemented the survey findings with expert input from Marsh & McLennan Companies (MMC) and RIMS.

We hope the insights gained from the survey and our expert analysis help further the debate on where issues lie, what needs to be done to address them, and what some good practices are.

Global and Emerging Risks – Definition and Characteristics[23]

Global and emerging risks are complex, usually exogenous threats and uncertainties that may have significant, unexpected impacts on company earnings and market positioning. As new phenomena or familiar challenges get sharply aggravated by changing conditions, they often take shape at the intersection of several fundamental trends and can quickly crystallize. Companies can be caught blindsided by spillover effects that cross geographic, sectorial, and other boundaries. For some such risks, there is no guarantee of a return to prior conditions, resulting in the emergence of a new status quo *(Figure 5)*. By and large, companies (individually or collectively), are not able to control such risks; they can only mitigate their exposures.

FIGURE 5

Challenges of global and emerging risks

SOURCE: MARSH & MCLENNAN COMPANIES' GLOBAL RISK CENTER

Systemic Risks

KEY FEATURES

- Correlated impacts with cascading/networked consequences

COMPANY CHALLENGE

- Anticipating scope of impacts

Emerging Threats

KEY FEATURES

- Complex interaction of drivers and no certainty of crystallization

COMPANY CHALLENGE

- Understanding significance

Shock Events

KEY FEATURES

- Larger magnitude than expected and likelihood only visible with hindsight

COMPANY CHALLENGE

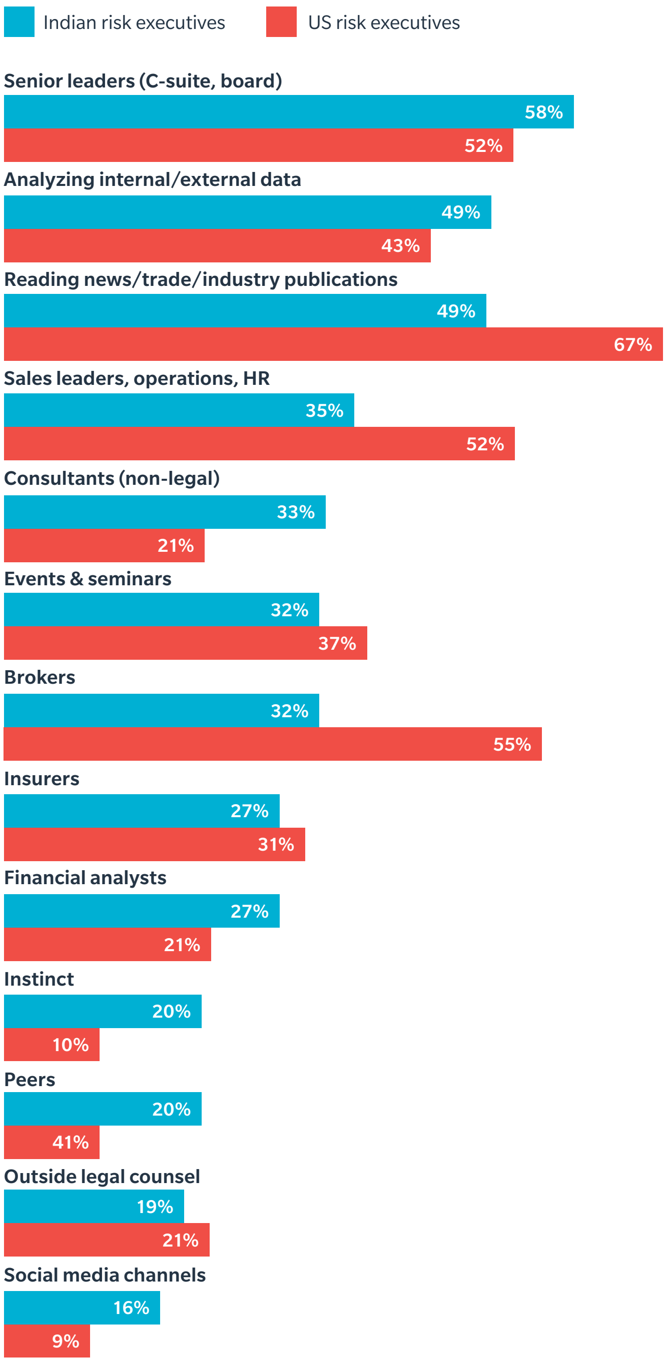
- Determining preparedness

Information on Emerging Risks Disseminated From the Top

The information sources that risk executives rely on to understand emerging risks can help us understand why forecasting is difficult, and provide us insights into opportunities for improvement. We asked Indian risk executives what they rely on to understand the impacts of emerging risks on their organizations and benchmarked their responses against the US 2016 survey results[22] *(Figure 6)*.

FIGURE 6

What sources of information do you rely on to understand the potential impacts that an emerging risk may have on your organization?



Two different styles of seeking for information are seen. On the one hand, Indian risk professionals display a more top-down, management-led style when disseminating information with most respondents choosing senior leaders as their top source of information (58 percent). On the other, US risk professionals take a more proactive, bottom-up style of sourcing for information. Their primary sources of information are news and industry publications (67 percent) as opposed to top management. Indian professionals can adopt the best practices from their US counterparts by subscribing to premier and readily available risk-focused information sources such as RIMS' RiskWire newsletter, Risk Management magazine, RIMS Risk Knowledge, and BRINK Asia - the digital news service of Marsh & McLennan Companies' Asia Pacific Risk Center.

Another major source of information for US risk executives is insurance brokers (55 percent), who understand current and emerging risks businesses face in different industries, making them an expert source of information. In India, however, only 32 percent of risk executives turn to their brokers for advice, illustrating that they should engage more with their brokers and tap on their wealth of information on emerging risks.

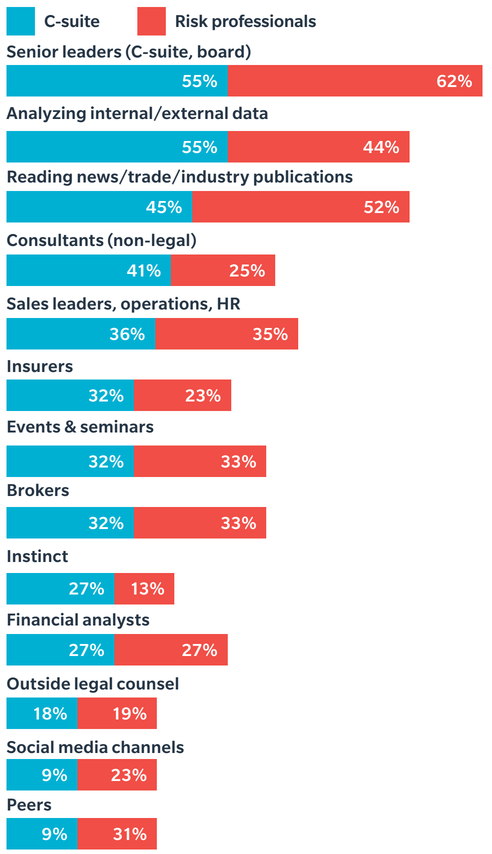
There is also a stark difference in how much information US and Indian respondents source from peers. While 41 percent of US risk executives communicate with colleagues or external peers on emerging risks, only 20 percent of Indian respondents do so. This highlights two possible scenarios: one being the lack of intra-organizational communication between risk executives, and the other a lack of engagement between risk executives and external peers from different companies and industries. It is therefore important to have organizations such as RIMS bring risk executives together via events and seminars to identify and benchmark best practices in risk management to benefit the larger risk community.

Additionally, risk executives in India could also make effective use of social media platforms to follow thought leaders and be abreast on the latest trends and reports around risk management.

Breaking down the information sources used by India's risk executives into C-suite and risk professionals *(Figure 7)*, we found that C-suite executives were noticeably more likely to rely on consultants (41 percent), insurers (32 percent) and both internal and external data (55 percent) than risk professionals. The message C-suites are conveying is clear: They are more likely than risk professionals in terms of seeking external professional perspectives.

FIGURE 7

Sources of information used by position in India



Surprisingly, just 9 percent of Indian C-suite executives get their information from their peers. This raises the question of why there is a lack of peer-to-peer information sharing, given that C-suite executives are usually better connected to high level industry experts and peers. Studying and discussing with peers across industries and companies can provide a holistic overview of potential risks to companies' leaders.

Looking across industries, the survey found that more regulated industries such as financial services and pharmaceuticals utilize more sources of information that other industries.

Indian Corporates Need to Adopt More Advanced Modeling Tools

After looking at the maturity level of Indian corporates in identifying risk, risk executives were asked about their organizations' methods in assessing and modeling emerging risks *(Figure 8)*.

FIGURE 8

Which risk management techniques does your organization use to assess/ model emerging risks?

A large number of survey respondents (51 percent) chose claims-based reviews. Organizations that use this technique rely on studying past incidents to try and predict how emerging risks will play out. Although there are benefits in reviewing claims, the effectiveness of this method is subject to the amount and quality of historic claims data available.

With advances in technology and analytics, there is an increasing number of advanced analytical tools and best practices available in the market providing a more comprehensive approach to evaluating emerging risks. They include performing a structured scenario approach and creating dynamic risks maps. The potential application of disruptive technologies such as artificial intelligence and machine learning can also help to better predict emerging risks, although they do come with their own risks.

Analyses developed by third parties such as consulting firms are the next most used risk management technique (38 percent). Risk consulting businesses that exist within insurance firms or insurance broking companies are uniquely positioned to help businesses analyze their risks because of their deep pool of claims, exposure, and placement data across industry, size, geography and product. The fact that organizations have to utilize the expertise of third parties again echoes the previous point, that Indian organizations are yet to reach their full potential in the ability to model emerging risks themselves.

Case Study

The use of claims-based reviews to assess top emerging risk concerns like cyberattacks and data breaches has its limitations, especially in the Asia-Pacific region. According to the MMC Asia Pacific Risk Center and FireEye,[24] this can be attributed to two factors:

- The lack of actuarial data. Cyber risk is a relatively new phenomenon as compared to longstanding risks such as flooding, and may have limited or no historic claims data available
- The low quality of actuarial data. Cyber insurance is still evolving based on the rapidly changing cyber landscape.[25] Coverage for cyber risks may have been packaged with other types of insurance, making it difficult for risk professionals to accurately isolate the impact of cyber threats on organizations.

Organizations can better quantify cyber risk by conducting a structured scenario approach. The process involves two broad phases: (i) identifying cyber risks, and (ii) quantifying cyber risks *(Figure 9)*.[26]

54%

Companies doing business in Asia that don't estimate the financial impact of a cyber incident

SOURCE: MARSH & MCLENNAN COMPANIES' ASIA PACIFIC RISK CENTER AND FIREEYE

FIGURE 9

Structured scenario approach to cyber risk quantification

SOURCE: MARSH & MCLENNAN COMPANIES' GLOBAL RISK CENTER

RISK IDENTIFICATION		RISK QUANTIFICATION	
IDENTIFY INSTITUTION-WIDE HIGH-VALUE ASSETS	IDENTIFY RISKS TO HIGH-VALUE ASSETS	ESTIMATE FREQUENCY OF CYBER RISK EVENTS	ESTIMATE SEVERITY OF CYBER RISK EVENTS
• Develop comprehensive list of cyber assets • Determine materiality of identified cyber assets • Create institution-wide list of high-value assets	• For each high-value asset, identify potential malicious actions • Assess potential threat vectors and state of existing controls • Identify most material cyber risks across institution	• Estimate frequency of cyber risk events, considering vector of attack, over a given time period • Supplement analysis with institutional data, simulated attacks, and expert opinion	• Use structured scenarios to quantify severity of cyber risk events based on loss types and loss drivers • Estimate severity of cyber risk event scenarios using distributions or point estimates of drivers

Organizational and Reporting Line Dynamics

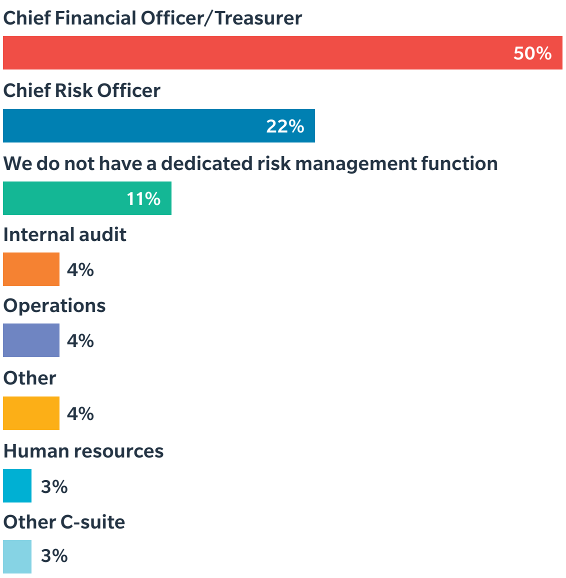
Reporting structures can complicate communication with senior leaders. Risk professionals were asked about their risk management reporting lines to understand how communication between risk management functions and their reporting body impacts the execution of risk management.

Most Risk Management Functions Report to the CFO or CRO

Most risk professionals reported having their risk management department reporting into the Chief Financial Officer (CFO)/ Treasurer *(Figure 10)*.

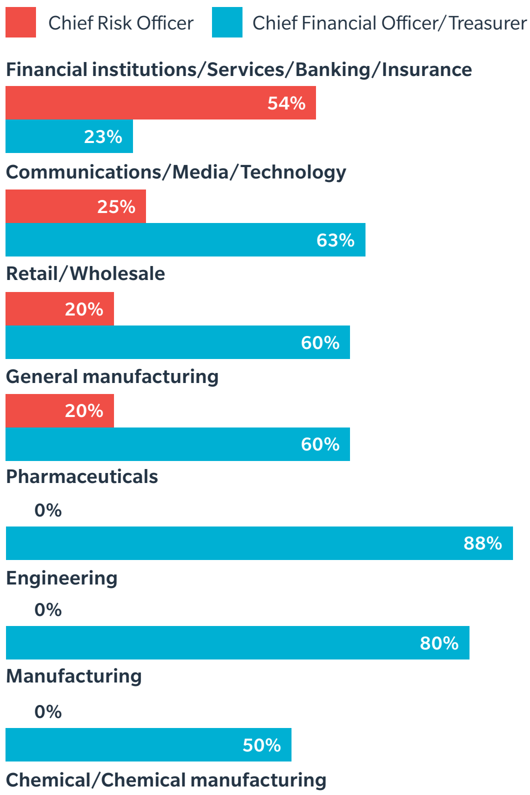
India has a significant proportion (22 percent) of its risk management function reporting to a dedicated Chief Risk Officer (CRO). This can be attributed to a recent regulation[27] passed by the Reserve Bank of India (RBI), India's central bank, that requires all banks to have a dedicated CRO position.

FIGURE 10 Where does the risk management function at your organization currently report into?



Looking across selected industries, financial services has the largest proportion of risk management functions reporting to a CRO (54 percent), with the next industry being communications, media and technology with 25 percent *(Figure 11)*. Interestingly, no survey participants from the pharmaceutical industry stated that their risk management function reports into the CRO. Instead, most of them report into the CFO/ Treasurer.

FIGURE 11 Risk management function reporting to Chief Financial Officer/ Treasurer and Chief Risk Officer by industry



Many Risk-related Functions Still Don't Have a Reporting Line to the Head of Risk Management

Respondents were asked which risk-related functions reported to the head of risk management *(Figure 12)*.

Several risk management functions such as compliance management and enterprise risk management had no discernible differences based on reporting lines. With increasing attention to statutory compliance like the revised Clause 49 of Securities and Exchange Board of India's (SEBI's) Equity Listing Agreement, regulators want boards to not only focus on value creation but also on value protection.

Other noteworthy perspectives include:

- Many respondents stated that IT risk management (61 percent) reports to the risk function, with 8 percent saying that they do not, but should. This is likely to grow in time because of the growing threat of cyberattacks that organizations are dealing with
- Just 36 percent of respondents stated that privacy management reports to the head of the risk function even though the industry has seen massive incidents of data fraud in recent times. This could be because privacy management in Indian companies usually falls under the purview of the IT risk management function. However, with data breaches becoming increasingly severe and Indian regulators bringing the country one step closer to having its own data protection law,[28] we can expect to see a greater emphasis on privacy management and a more involved role of the second line of defense on data privacy risk
- Another crucial component of the risk function other than identifying and assessing risk is to transfer risk away from the organization. Part of the insurance management's function is to do that. A majority (62 percent) of Indian companies have their insurance management function reporting to the head of risk, which is a good sign given the increasingly volatile business environment. However, as compared to the US,[29] where 92 percent respondents say that their insurance management function reports to their head of risk and only 7 percent don't, the situation in Indian companies can be improved
- Less than half of the respondents said that supply chain risk management (48 percent) and environmental risk management (44 percent) report to the risk management department; and almost a third of respondents for both functions say that they do not report to the risk management team either. This is surprising given the severe business disruptions India has faced from critical risks like extreme weather conditions that have devastated supply chains and the environment

FIGURE 12

Which risk-related functions currently report into the head of the risk management department?

Risk Management Effectiveness

Finance and human resource executives frequently work with capital allocations, budgets, and employee performance targets to align individual goals and corporate strategies. We looked at how risk management operations employ similar practices as they seek greater focus on improved execution of risk management priorities.
The results were viewed through three lenses:

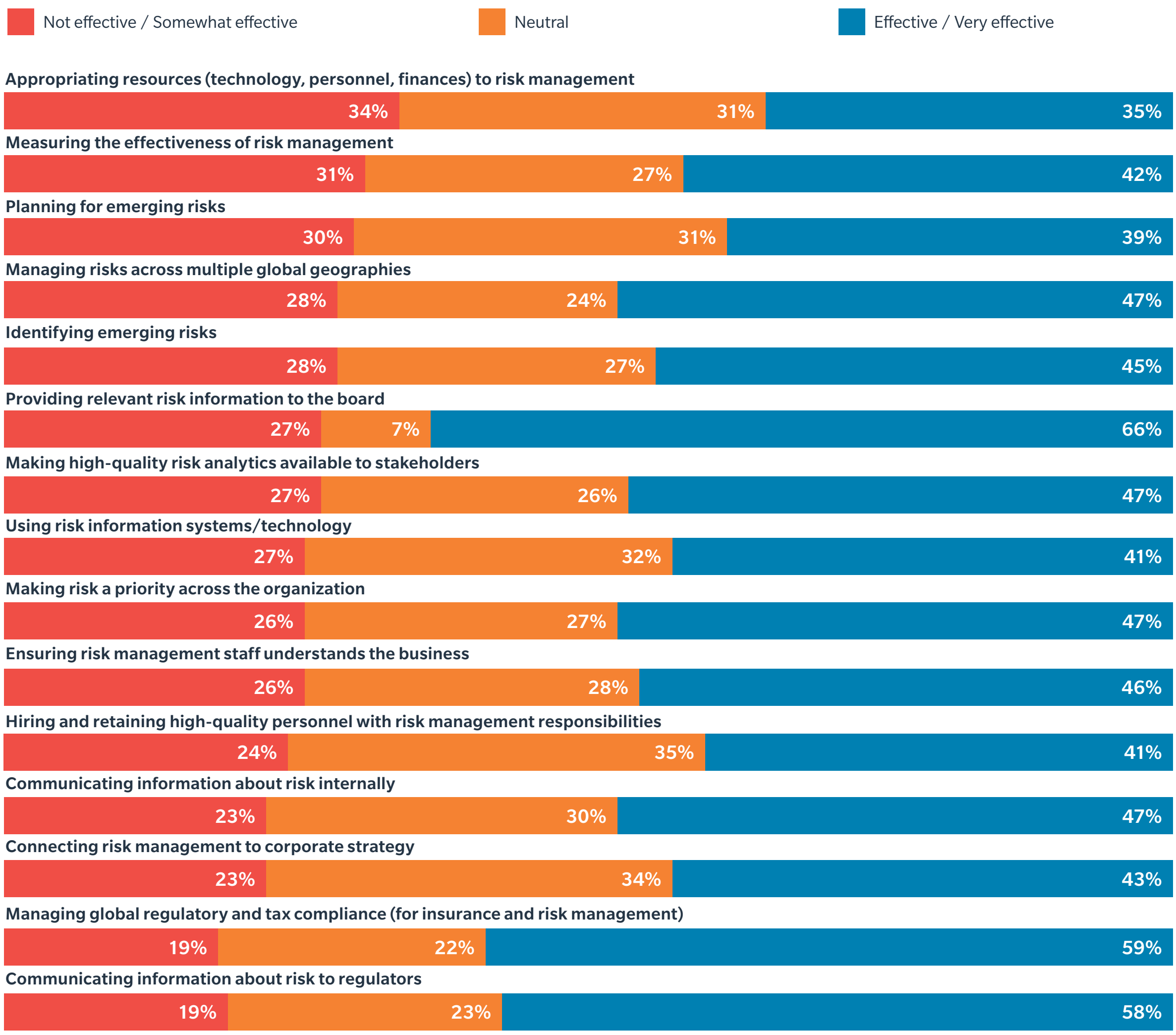
1. How effective are organizations in key risk management activities?
2. How effective are organizations in collaborating with various organizational functions on key risk management protocols?
3. What performance standards are used to measure effectiveness and organizational alignment?

Significant Improvement Required Across Risk Activities

Respondents were aske to rate their organization's effectiveness in several risk-related activities. The results highlight a startling ineffectiveness across almost all organizational activities relating to risk. More than half of the responses across all areas either state that they lack effectiveness or are neutral about it *(Figure 13)*.

FIGURE 13

How would you rate the effectiveness of your organization at the following activities as they relate to risk?



More needs to be done by organizations particularly in areas such as:

Appropriating resources (technology, personnel, finances) to risk management. This area not only saw the lowest effectiveness rating (35 percent) by respondents but the highest ineffectiveness rating (34 percent) as well. C-suite executives generally reported more effective ratings as compared to risk professionals *(Figure 14)*.

FIGURE 14

Appropriating resources to risk management by position

Measuring the effectiveness of risk management saw only a 42 percent effectiveness rating and corroborates with organizations' ineffectiveness in appropriating resources, because quantifying the risk function's value is essential when senior management makes its case for yearly budget allocations to the board.

Other areas with dismal results were in identifying emerging risks and planning for emerging risks, which saw effectiveness ratings of 45 percent and 39 percent respectively. When comparing across organizations, larger organizations report being more ineffective in identifying and planning for emerging risks as compared to smaller firms. This confirms that even larger Indian organizations have difficulty in forecasting and assessing emerging risks.

Some areas were effective, such as providing relevant risk information to the board (66 percent). This is expected since a large proportion of risk management functions in corporate India report to the CFO/ Treasurer (50 percent) or a dedicated CRO (22 percent) (Figure 11) who have access to the board. However, how essential is risk reporting to the board?
This again implies that most risk executives rely on senior leaders including the board of directors as their source of information for emerging risks, rather than being proactive in seeking information on their own.

According to the US 2015 survey,[29] there was a much higher effectiveness rating across more than half the areas in the US as compared to Indian responses. Areas in which Indian organizations saw difficulty, such as allocating resources and identifying emerging risks, saw US organizations faring better.

Collaboration Across Functions

Most risk executives understand that actual risk management takes place within the day-to-day operation of the enterprise. Therefore, deploying best practice risk management protocols across the enterprise is a central requirement.

Survey participants were asked how involved various parts of the organization are in four key risk management protocols:* risk committee participation, risk management strategy development, risk assessments, and risk response:

Risk committees: Representation from environmental risk management and public relations is noticeably absent from corporate risk committees, although internal audit and compliance management played prominent roles.
This is aligned to the increasing regulatory pressure organizations face.[30]

Risk management strategy development: The top three areas identified as being involved in risk management strategy development were strategy development, public relations/ communication, and information technology and network. First, it is encouraging to find that the strategy function is most involved in developing risk strategy as it displays resolve by Indian organizations to integrate risk management into overall firm strategy. Second, more is being done by organizations to address public relations from its lack of representation in risk committees and in risk response. And lastly, as ever changing cyber threats are posing huge risks to organizations now, it is not surprising to see information technology and network as part of the risk management strategy development.

Risk assessments: Quality control/ product management, information technology and network, and business units/ operations/ production were the top three areas identified as being involved in risk assessment. That information technology and network comes out on top again points to organizations' reliance on it in driving the business engine.

Risk response: This reflects a post-event "damage control" perspective, rather than an emphasis on developing alternative responses for avoiding or preventing losses or, when feasible, exploiting a risk. From a risk response standpoint, the top three areas cited were business units/ operations, security management, and safety management. It was surprising not to find public relations as a top area since their function is usually heavily involved in the "damage control" process. In fact, public relations seem to be the function most lacking in Indian organizations, with 29 percent respondents not even knowing whether it is involved in any of the four risk management activities.

*Organizational functions listed in the survey were: Actuarial; business continuity/ crisis management; business units/ operations/ production; compliance management; environmental risk management; executive management; finance/ financial planning/ treasury; human resources; internal audit; information technology and network; legal; public relations/ communication; quality control/ product management; research and development/ innovation; safety management; security management; and strategy development.

Measuring the effectiveness of the risk function

Faced with an uncertain risk landscape and a renewed focus on value protection by boards, there are increased expectations on risk management and an increased involvement of it in business strategy. With this evolution, it becomes even more important to be able to measure risk management's effectiveness, and to do so in ways that reflect the change.

After seeing many respondents state the ineffectiveness of organizations in measuring the effectiveness of risk management, we look at what measures organizations actually use to quantify it *(Figure 15)*.

Most risk management departments in India report being evaluated on timely risk identification, assessment, and reporting; responses from the US 2015 survey[29] echo that same result too. Other than that, risk management departments in the US also rely extensively on traditional measures such as claims management results (72 percent) and insurance budgets (74 percent).

It is encouraging to see risk executives in India are prioritizing measures such as integration with operations (39 percent) and impact on strategy development and execution (35 percent), as compared to more traditional measures like claims management results (24 percent) and insurance budgets (11 percent).

FIGURE 15

Which of the following does your organization use to measure the effectiveness of the risk management function?

Priorities for Improving Risk Management Capabilities

Lack of Expertise in Modeling Emerging Risks Poses a Challenge to Businesses

A large part of why most risk executives do not understand the impact of emerging risks is their lack of know-how in modeling the magnitude of emerging risks *(Figure 16)*. Furthermore, there are unique challenges in quantifying emerging risks. Take cyber risks for example – the lack of historical data, a rapidly changing threat environment where attackers are constantly finding new attack vectors, and non-standardized cyberattack outcomes make quantifying the impact difficult.[26] This means that companies do not adequately understand the impact of emerging risks on organizational strategy, and in the decision-making process even if they know what the risks are.

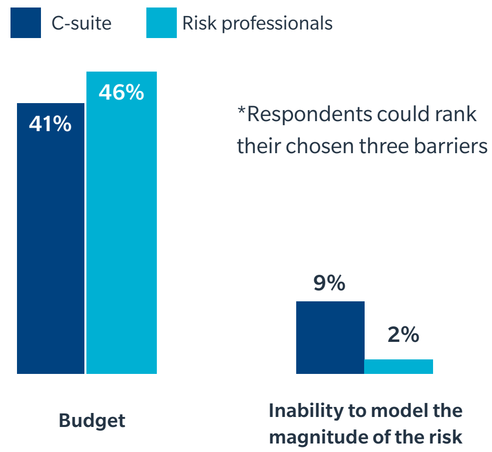
FIGURE 16 What barriers inhibit your organization’s ability to understand the impact of emerging risks on business strategies and decisions?

This lack in risk quantifying capability is especially detrimental to the risk function when risk executives go to the board asking for a budget to address specific risks.

As the risk environment becomes increasingly complex and more entwined with financial decisions, risk strategy is increasingly becoming a boardroom issue. The budget approved by the board for risk management is critical in an organization’s risk management strategy. While budgetary constraints are not as pressing an issue in the US[31] and Latin America[32] with respondents not listing it as a top five barrier to risk management, in India, budgetary issues took the top spot as the largest barrier (45 percent). This implies that there is significant room for Indian organizations to increase and better allocate their budget as compared to US and Latin American organizations.

When looking across positions, both C-suite and risk professionals placed budgetary constraints as the top barrier compared to the inability to model risk in India *(Figure 17)*. This highlights the potential lack of alignment between the C-suite or CRO and the board of directors on their priorities for the organization around risk management.

FIGURE 17 Top ranked* barrier chosen by C-suite and risk professionals



*Respondents could rank their chosen three barriers

Top five steps for communicating with executives

1. Prepare for the meeting
2. Listen carefully
3. Speak their language
4. Propose solutions
5. Challenge yourself

SOURCE: RIMS

Misalignments within the organization are a challenge as well. Symptoms of it show through an organization's lack of awareness of key risk management concepts, the lack of support and communication from senior executives, and the increasing siloes seen from the lack of cross-organization collaboration. All of these inhibit an organization's ability to understand the impact of emerging risks on business strategies and decisions.

RIMS has observed in the US that misalignment within the organization can be addressed by risk managers adopting communication styles that resonate with executive management.[33] They need to make sure the information they're presenting is actionable and directly related to business priorities and overall strategy. If done well, this can lead to executive management starting to request risk management input into key issues.[34]

Data and Analytics are Essential in Quantifying Risks

Questions about data and analytics have been asked in prior Excellence in Risk Management surveys in the US, and there has been a consistent call to improve their use. For example:

- In 2011, improving quantification and analysis of risk was among the top three areas where senior management's expectations of risk management had grown
- In 2015, improving quantification of risk was the top area that risk executives believed would benefit their organizations through its use of data and analytics

In 2018, this trend is evident in India. When asked where they would like to improve the use of data and analytics *(Figure 18)*, respondents were overwhelmingly in favor of quantifying specific risks, including emerging issues (80 percent). This reinforces the trend for organizations both in developing and developed geographies to seek additional support in the form of resources, tools, experience or knowledge for decision-making processes based on data and analytics.

FIGURE 18 My organization would benefit by improving its use of data and analytics in the following areas*

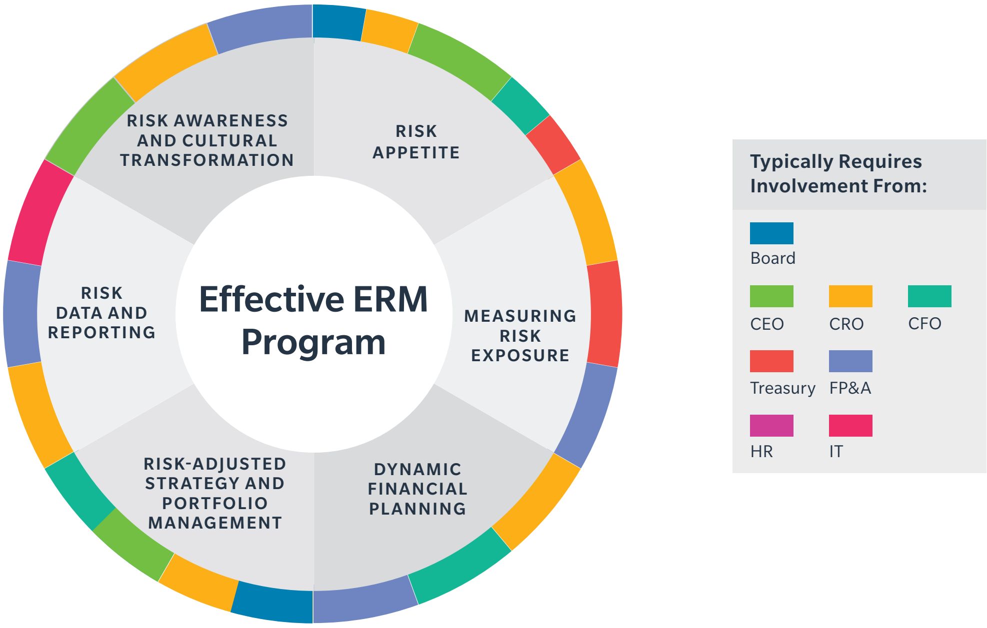
*Respondents could choose three from the list

Upgrading Technologies and Putting a Strategic Focus on Risk Management are Among Top Focus Areas

Today's disruptive technologies will soon be—and in many cases already are—the norm for doing business. Furthermore, data is a crucial factor and will become even more critical in the future for businesses to tap into, allowing them to make effective risk decisions.

FIGURE 19 Six building blocks of an effective ERM program

SOURCE: MARSH & MCLENNAN COMPANIES' GLOBAL RISK CENTER



As disruptive technologies and large amounts of data change business models, risk executives should actively engage key stakeholders – from senior leaders to operations employees to suppliers – in developing risk management capabilities and using the insights in business strategy decisions.

The top five focus areas that Indian risk executives chose for developing their company's risk management capabilities in 2019 are:

- Upgrade risk management technology and access to information
- Integrate enterprise risk management into strategic planning
- Improve the use of data and analytics
- Improve risk governance structure
- Formalize risk management training/education across the organization

The integration of enterprise risk management (ERM) into strategic planning is essential for an organization's long-term viability. ERM is a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.[35] To conceptualize ERM, the MMC Global Risk Center recommends breaking it down into six building blocks *(Figure 19)*.

ERM is an essential part of creating and maintaining operational efficiency, developing organizational resilience, and adding economic value. Integrating ERM into an organization's strategy boosts risk responsibility from top management, deepening their organizational awareness of risks and continuous participation in solutions.[36] Studies published by RIMS have shown that, based on the RIMS Risk Maturity Model, mature practices of ERM can lead to a 25 percent boost in firm valuation.[37] At RIMS.org, risk managers can find the RIMS Risk Maturity Model online diagnostic tool to begin their ERM maturity measurement and benchmarking.[38]

Improving the risk governance structure is also a top focus area for most risk executives. The National Association of Corporate Directors (NACD) recommends that boards build proficiency in the use of adaptive governance.[39] Adaptive governance comprises:

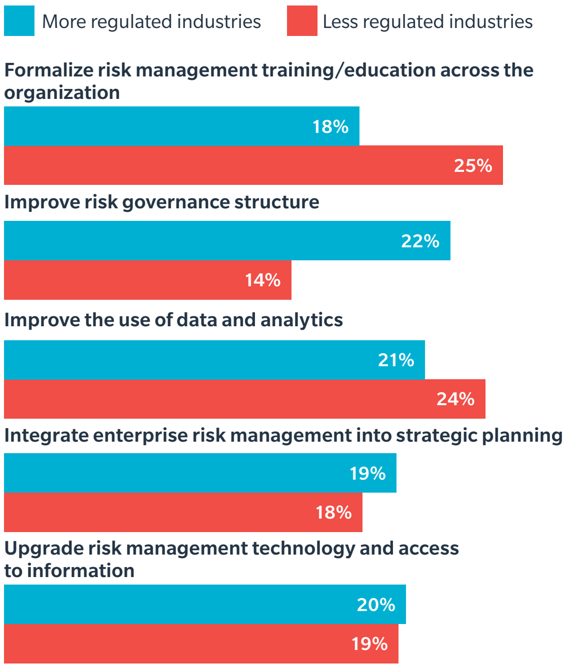
- Active involvement by directors in setting and maintaining a boardroom culture that is centered on open discussion, constructive challenge, and active self-reflection
- Board skills that remain fit for purpose in a rapidly evolving business environment
- Dedicated time on board agendas to look at the organization's future, including discussing the potential for disruptive risks to affect long-term strategy and value creation
- The board taking an active role in guiding the organization toward improvements in resiliency

This allows directors to aid the management team by helping the organization see around corners.

When looking across industries by their extent of regulation,* both regulated and lesser regulated industries had similar results across most dimensions except on improving the risk governance structure and formalizing risk management training across the organization *(Figure 20)*. More regulated industries will be focusing on improving their risk governance (22 percent), compared to less regulated industries (14 percent). However, less regulated industries are also trying to better formalize risk management training across their organization (25 percent) and improve their use of data and analytics (24 percent).

FIGURE 20

Focus areas for developing your company's risk management capabilities in 2019 across extent of regulation on industries



* More regulated (from a risk management perspective) industries include: Aviation, Power and Utilities, Chemical/ Chemical Manufacturing, Communications/ Media/ Technology, Pharmaceuticals, Engineering, Financial Institutions/Services/Banking/Insurance, transportation, Energy. Less regulated industries include: Agriculture, Education, Mining, Metals, and Minerals, Automotive, Construction, Food and Beverage, Professional Services, Diversified, General Manufacturing, Retail/ Wholesale

Across industries *(Figure 21)*, more regulated industries such as energy, chemical/ chemical manufacturing and finance are looking to increase their risk governance structure while less regulated industries such as construction, and diversified and manufacturing companies are looking to formalize their risk management training across their organizations.

FIGURE
21
Focus areas for developing your company's risk management capabilities in 2019 across industries

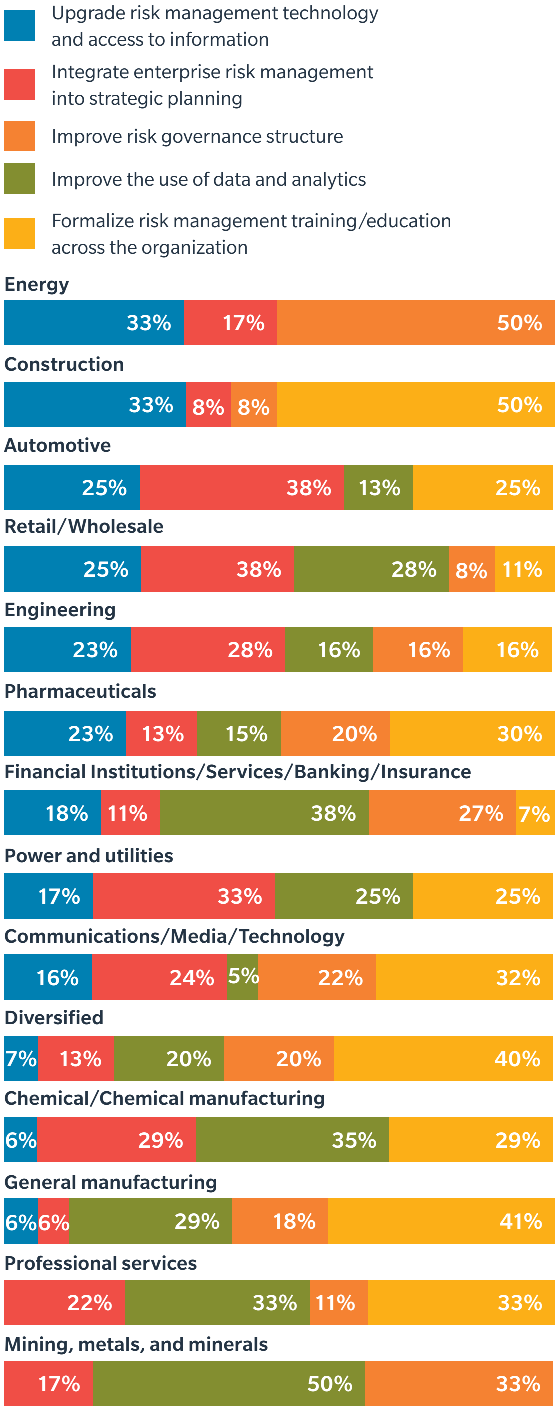
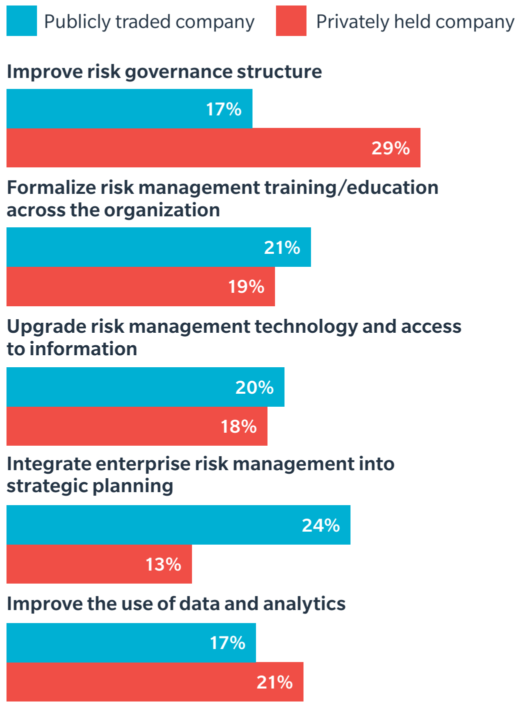


FIGURE
22
Focus areas for developing your company's risk management capabilities in 2019 across organization type



Currently, corporate governance regulations and frameworks are in place especially for listed companies that use the SEBI Listing Agreement guidelines. We aimed to unearth any distinct focus areas between public and private organizations in India *(Figure 22)*, and two clear differences appeared. First, private companies plan to focus heavily on improving their use of data and analytics (29 percent) as compared to public companies. This highlights more focus on increasing their risk quantification capabilities, and also implies that public companies are slower in adopting such technologies, which could be owing to greater organizational red tape as compared to private companies.

Second, public companies are planning to formalize risk management training (24 percent) across their organizations much more than private organizations (13 percent). With increasing scrutiny by boards in ensuring that the value of a company is protected, formalizing risk training across organizations is a foundational component[36] of their risk culture, not only helping mitigate risk across the organization but also enhancing its overall performance.

Investing to Foresee Emerging Risks

After understanding some challenges that Indian companies face and where their focus lies, it is imperative to look at how organizations will be investing in their risk management-related functions *(Figure 23)*. Will they expect to see investments in areas they have highlighted as being key to their organization?

The previous section on focus areas found that risk executives are looking to concentrate their efforts on upgrading their organization's risk management technology, formalizing risk management training across the organization, and improving the use of data and analytics. This is aligned with the expected increases in investment in similar areas.

- Seventy-two percent of respondents expect to see an increase in investments for risk management training. Firms can invest in employee risk management training by sending them to internationally approved and certified programs like the RIMS-Certified Risk Management Professional certification
- Sixty-six percent of respondents expect to see an increase in investments toward risk management information systems
- Sixty-four percent of respondents expect to see an increase in investments toward risk analytics

Not only do they expect investment to increase in the above-mentioned areas, but none of the respondents expect to see any decrease in investments.

FIGURE 23

For each area below, do you expect your level of investment over the next two years to:

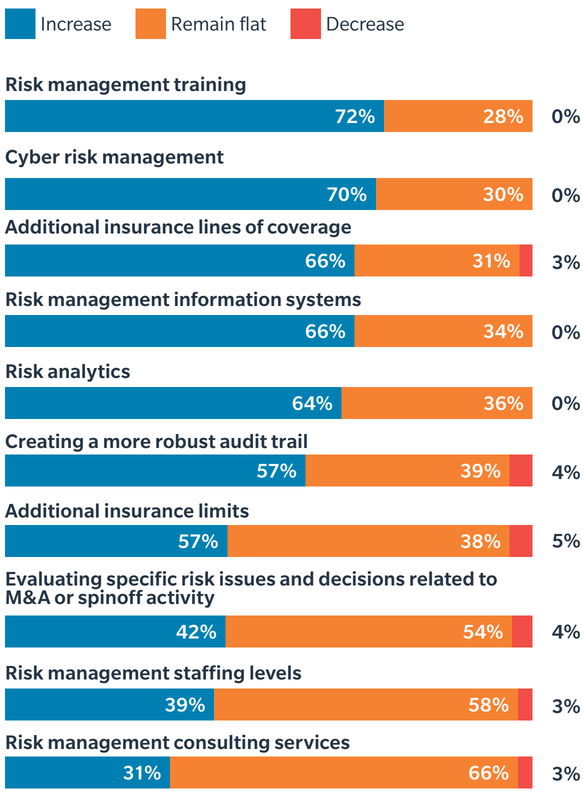
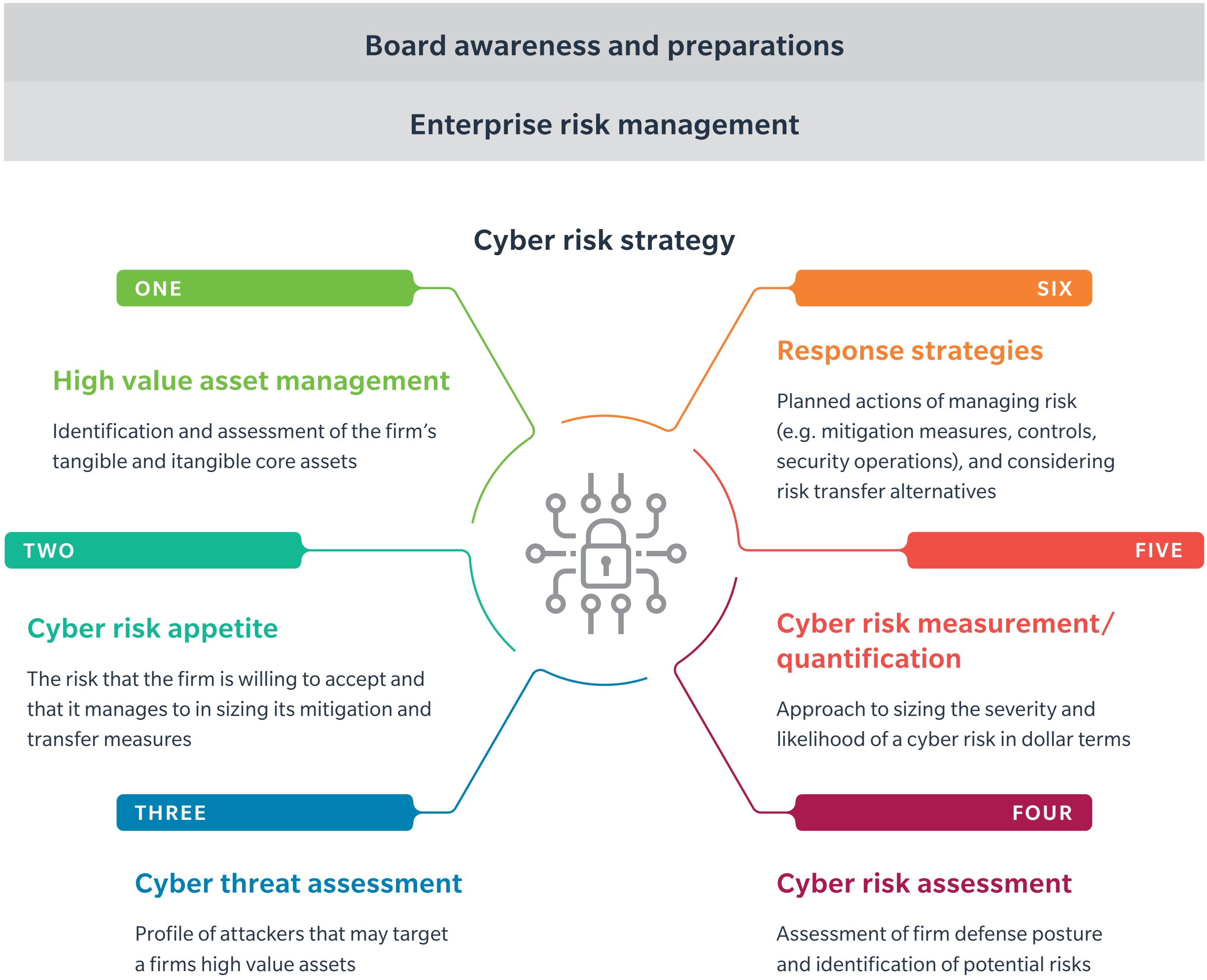


FIGURE 24

Focus areas of a comprehensive cyber risk management process

SOURCE: MARSH & MCLENNAN COMPANIES' GLOBAL RISK CENTER



Cyber risk management is also a key focus area with 70 percent of respondents expecting an increase in investment, which is aligned to cyberattacks being chosen as the top risk. The same results were found in the US 2016 survey,[22] in which 77 percent of respondents expected investment for cyber risk management to increase. Organizations can improve cyber risk management by adopting six key focus areas of a comprehensive cyber risk management process, according to a report by MMC Global Risk Center and the Women Corporate Directors[40] *(Figure 24)*.

Strategies to Advance Risk Management Capabilities

A fundamental factor in having successful risk management capabilities observable through this study is organizational culture. By learning what strategies are necessary to advance risk management capabilities, a firm can facilitate the internalization of this organizational culture *(Figure 25)*.

- The integration of risk management with the strategy and values of the organization is the top strategy for 81 percent of risk executives. This is for the transformation of their organizational culture to be more risk management-oriented. One way to encourage integration is through systematic reporting and linking risk management to performance measurement and strategic indicators
- Coming in second at 72 percent, risk management as part of day-to-day business is also a great facilitator in advancing risk management capabilities
- It is also imperative that risk management initiatives are communicated effectively, and training is conducted regularly for both new joiners and experienced staff. A complete communication strategy is required, which includes the identification of different audiences (internal or external), key messages that are to be imparted, environment, periodicity, and, of course, what measurement instrument will be used at the end of this strategy to measure its effectiveness. Any process of cultural transformation within an organization must be gradual – a consistent message must be given and be adequately reiterated for it to achieve the expected impact. Therefore, raising awareness through effective and measurable communication strategies is one of the main points for risk management leaders in India

FIGURE 25

What strategies do you find necessary to transform the culture of your organization to be risk management oriented?

Adoption of New Technology

Many Organizations Still Need Risk Processes Around New Technology

A changing risk landscape isn't new for risk professionals who have long dealt with emerging risks, ranging from cyberattacks and climate change to floods and fiscal crises. Emerging technologies are impacting major industries globally *(Figure 26)* and are shaping how businesses are run. They empower businesses in many areas like operations and risk management – for instance, Marsh's recent collaboration with IBM has enabled Marsh to provide blockchain proof of insurance to its clients.[41] However, disruptive technologies like blockchain also carry their own set of risks and require an effective framework to be successfully implemented.[42]

FIGURE 26

Impact of emerging technologies on major industries

SOURCE: INDUSTRY REPORTS, MMC GLOBAL RISK CENTER ANALYSIS

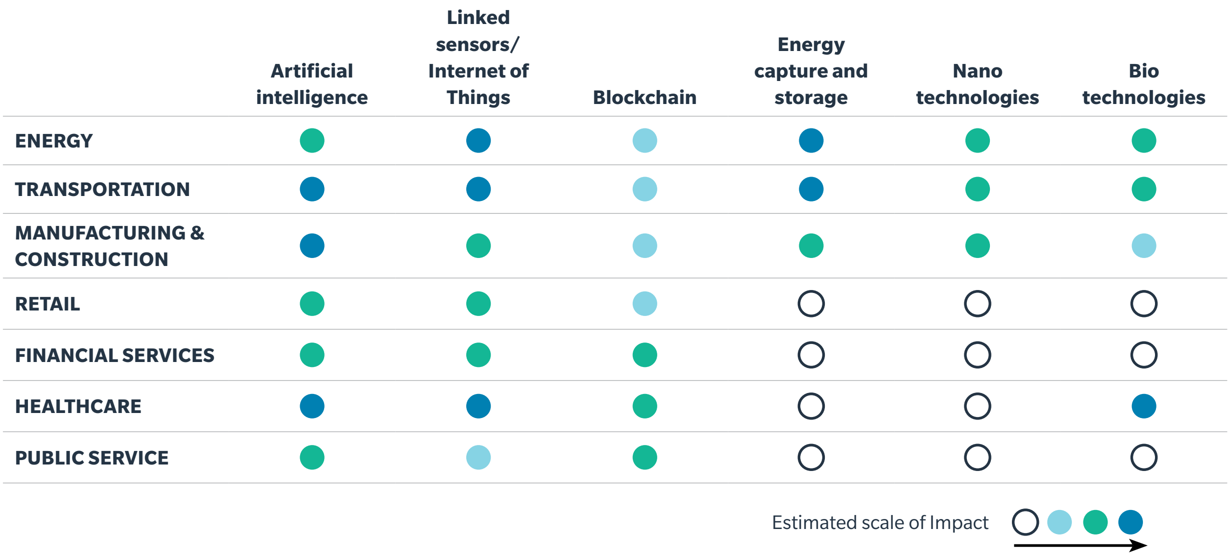
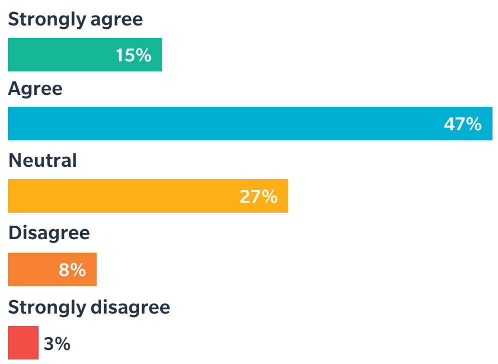


FIGURE 27

There is a clear process at my organization for identifying and addressing potential risks when considering and implementing emerging technology



How well are Indian organizations positioned for the impacts of disruptive technology and the rapid pace of innovation?

Companies are generally uneasy about the way they address the risks of disruption. Just 15 percent of respondents said they "strongly agree" that their organization has a clear process in place for addressing risks associated with disruptive technology *(Figure 27)*. Nearly four in 10 risk executives in India could not say there is a clear process at all.

When comparing the industry impacts and whether industries have clear processes on handling emerging technology *(Figure 28)*, a few key points stand out:

- Financial services face quite a significant impact from emerging technologies. However, although a majority of respondents (54 percent) from the financial services have clear processes, it is much lower than in other industries. For one, banks in India lag in terms of adopting technologies and the processes around them. This sentiment was echoed by the former governor of the RBI, Raghuram Rajan, who acknowledged the inadequacy of Indian banks in adopting new technologies.[43] The RBI has itself also been lagging in this area. Only a few months ago, it formed a new unit to research, and possibly draft rules and supervise new emerging technologies like blockchain and artificial intelligence in the Indian financial sector[44]
- Forty percent of manufacturing respondents said they do not have clear processes around emerging technology. This is startling because emerging technologies like artificial intelligence are already shaking up the industry, automating many processes within the manufacturing value chain.
- Although the retail/ wholesale industry is utilizing more emerging technologies—from artificial intelligence and machine learning in shopping apps to the use of Internet of Things in cashier-less stores[45]—60 percent of retail/ wholesale respondents do not have clear processes around such technologies.

To get around this, firms can utilize regulatory sandboxes, which not only encourage innovation but ensure oversight as well.[46] For instance, the RBI is working on forming a regulatory sandbox for fintech and setting up data science labs to keep pace with innovation in the digital lending space.[47]

The difference in findings on the basis of the size of risk management teams were as expected – companies with larger and more established teams reported having clear processes around identifying and addressing potential risks from emerging technology compared to smaller risk management teams *(Figure 29)*.

FIGURE 28

There is a clear process at my organization for identifying and addressing potential risks when considering and implementing emerging technology across industries

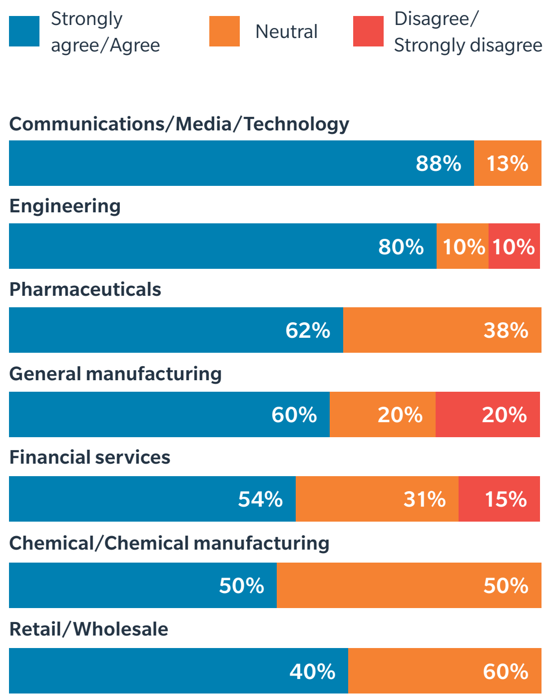
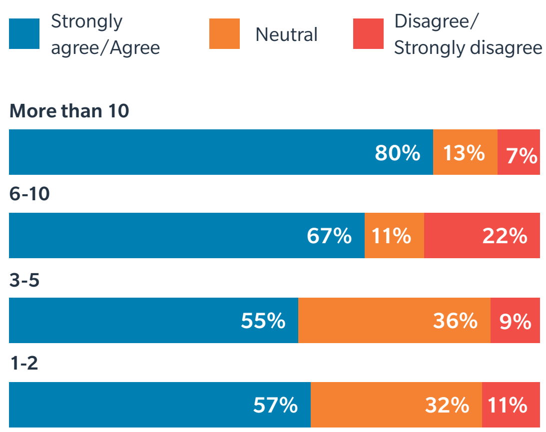


FIGURE 29

There is a clear process at my organization for identifying and addressing potentaial risks when considering and implementing emerging technology across risk management team size



Aiming for a Strategic Grasp of Disruptive Technologies

Disruptive technologies bring about unique risks that are increasingly becoming interwoven in industries and markets.

Risk professionals generally do not need to understand the detailed intricacies of how every new technology impacts risk management. However, they do need to understand the technologies and their strategic uses within their organizations because only then can they appreciate the associated risks and treat them accordingly.

Risk professionals also need to get used to talking to technologists to understand which technologies are being used in their organizations, how they are being used, and whether some can be leveraged to improve how organizations manage risks. The potential impacts of not being able to do so include being left out of decision-making, failing to foresee and develop required modifications, and falling out of step with advances in the risk management profession.

Our survey focused on three new disruptive technologies – artificial intelligence, blockchain, and the Internet of Things – that are already impacting and will continue to impact risk management. Overall, although a majority of survey respondents (66 percent to 72 percent) had an awareness of these disruptive technologies, only a handful felt that they could translate their knowledge into contributions or to utilize it at a "strategic advisor" level *(Figure 30)*.

Benchmarking India's survey responses to the US results from 2018 *(Figure 31)*,[48] it was found that Indian organizations lack strategic advisors on the topic of disruptive technologies as compared to US organizations, highlighting that there is still room for corporate India to transform its awareness into strategic contributions to their organization. Perhaps when more Indian organizations start focusing on identifying and assessing potential emerging risks from disruptive technologies and integrating them into their business strategy, they will be able to emulate their US counterparts in contributing strategically to their organization.

How knowledgeable is the risk management function at your organization regarding the impact of the following technologies on business and risk?

FIGURE 30 Responses in India

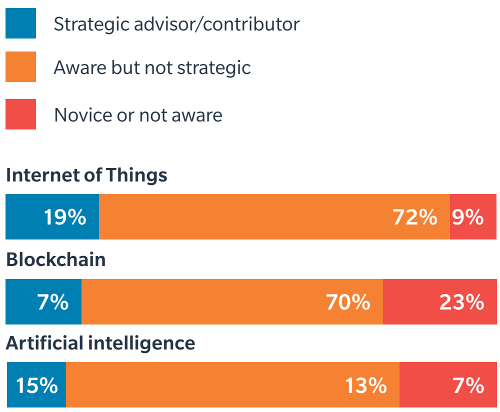
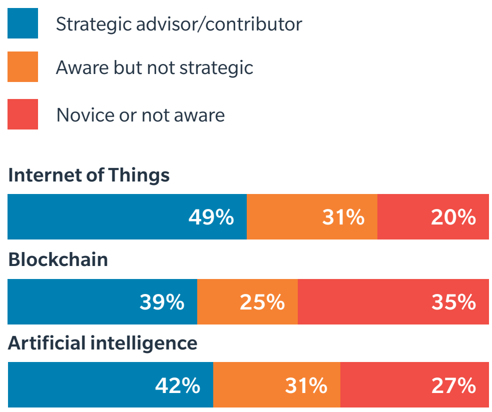


FIGURE 31 Responses in the US



Conclusion

Large scale cyberattacks, severe incidents of data breaches, and severe weather events are just a few of the many emerging risks that will affect the business environment in India. The interaction of longstanding and emerging risks is creating even more unique and unpredictable risks in a manner that is making it hard for organizations to even identify risks.

Indian organizations—and especially their risk functions—need to be prepared to face such risks. Our survey indicates that more can be done by organizations in identifying, assessing, and quantifying risks. Organizations need to be more proactive in keeping up to date about emerging risks. They can do this through greater interactions with their brokers and by participating at events and forums where risk management knowledge and best practices are shared. Upgrading risk assessment methods should be a priority given the rapidly changing risk landscape.

Many risk management teams in India report directly to a CFO or CRO. This is heartening to see as it shows a direct line of communication on risks to top management, keeping them abreast of any developments on emerging risks, and allowing them to communicate this to the board effectively. However, when it comes to the effectiveness of their risk management activities, much more can be done, especially in areas such as measuring risk management effectiveness and resource appropriation.

The inability to model risks and budgetary concerns are the top barriers Indian organizations face. They are highly correlated with the management not being able to make a successful case for their risk management budgets because they cannot justify it. As such, key priority areas for organizations to improve their risk management capabilities include upgrading risk management technology and access to information, and improving their use of data and analytics (both highly critical tools when quantifying risks). It is also crucial for organizations to ensure that risk management integrates with the strategy and values of the organization, and then set it in stone by implementing risk management processes within the day-to-day business.

Disruptive technologies are shaping the way businesses operate, and they carry both the ability to empower or weaken organizations if not used wisely. Many businesses in India are still largely uneasy about how they address risks associated with disruptive technologies. However, in industries that face greater regulation, more positive results are seen. Regulators can provide the impetus for businesses to adopt clear frameworks around such technologies.

More needs to be done by corporate India to meet the new challenges arising from the intersection of risks. Organizations need to be more effective in risk management activities. Risk executives need to understand the challenges their organization faces and then focus on key areas to improve their risk management capabilities. Only then, will they be ready to face an increasingly complex, interconnected and volatile business environment.

Recommendations

Identifying, assessing and preparing your organization against potential impacts of emerging risks are key responsibilities of risk executives. With proper insight, planning and implementation, it can provide organizations opportunity and a competitive advantage. Here are a few recommendations for consideration:

Develop a clear understanding of what senior management expects from the risk management department

The C-Suite wants risk managers to be well-versed in the workings of their organization and its industry.

They also expect risk managers to possess a strategic view of risk and put in place a Risk and analytical framework which can guide the organization to successful strategic outcomes.

Educate yourself

Be conversant in the leading-edge innovations in your industry and in others'. Pay attention to hits and misses and emerging risks, especially around those technologies your organization is using or planning to use.

Engage your brokers, it is their job to understand the risk landscape for their clients.

Keep up to date with risk related news and publications by following leading thought publications like RIMS RiskWire, Risk Management magazine, RIMSCast, RIMS Risk Knowledge, BRINK Asia and the Marsh & McLennan's Global Risk Center.

Expand your network and foster collaboration

Build cross-functional relationships inside your organization. Develop strategies to increase alignment regarding risks and risk management across the organization.

Study and confer with experts outside of your industry to better understand how disruptive technology may shift your risks. Premier organizations like RIMS provide opportunities through events and peer-produced education for you to do so. Their mission is 'To educate, engage and advocate for the global risk community."

Push for investments

Begin to develop a "value proposition" for risk management in your organization if you have not done so already. Use it to connect with organizational objectives and strategic thinking and to bring new and improved ways to detail the contribution risk management makes to the organization.

Learn which data and analytics tools will help you dig deeper into your company's risk issues; then make a case for investing in them.

Ensure you hire people with the right skill sets to keep you on the leading edge.

Consider the wider impacts of disruptive technology

Acknowledge that technology is bringing change to your organization and to the risk management profession.

Anticipate and comprehend the impact of disruptive technology risk in your industry and on your business operations.

Use "cyber risk" as a wedge issue to draw attention and examine a variety of risks related to disruptive technologies.

Continue to break down organizational silos

Challenge the agenda of your organization's risk committee. Does it include a review of broader trends and the potential emerging risks in its governance framework?

Discussions around emerging risks should be a regular feature, not a once-a-year exercise.

Get out of the office when possible and see how your company does business.

Demonstrate the value of Risk Management, beyond insurance and claims cost reductions.

Survey Demographics

FIGURE
32

Please select the title below that most closely describes your current position

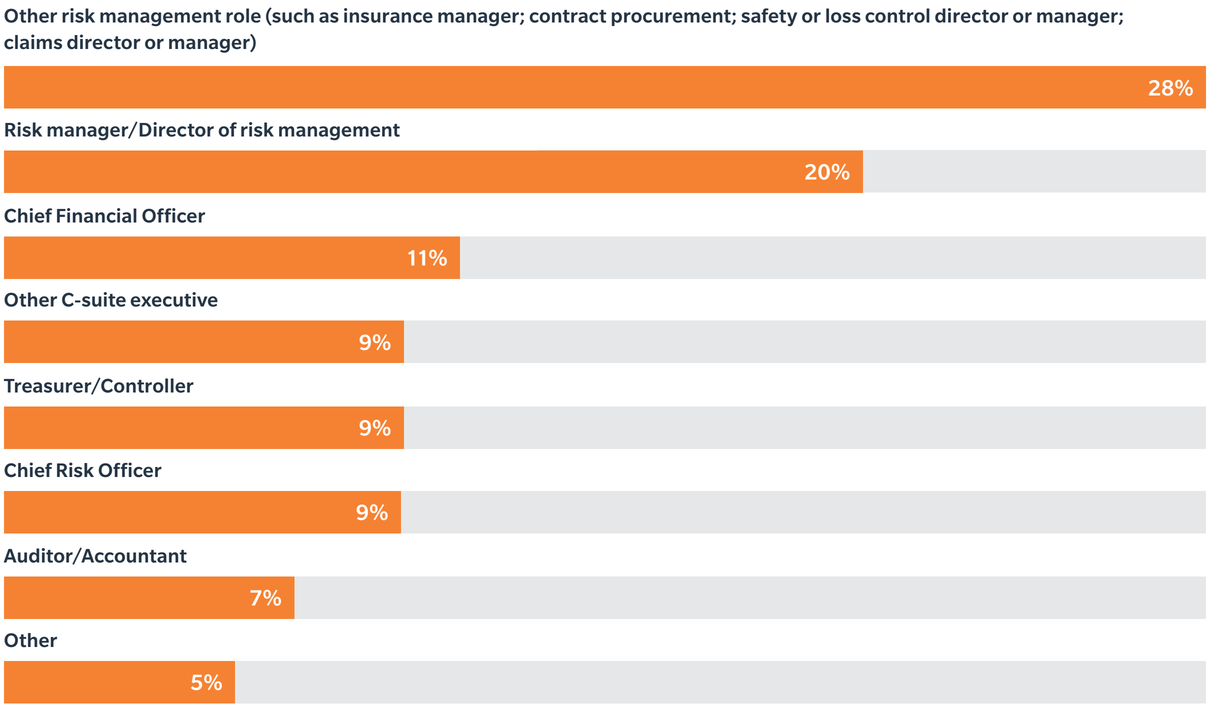


FIGURE
33

What is your organization's annual revenue in Indian Rupee?

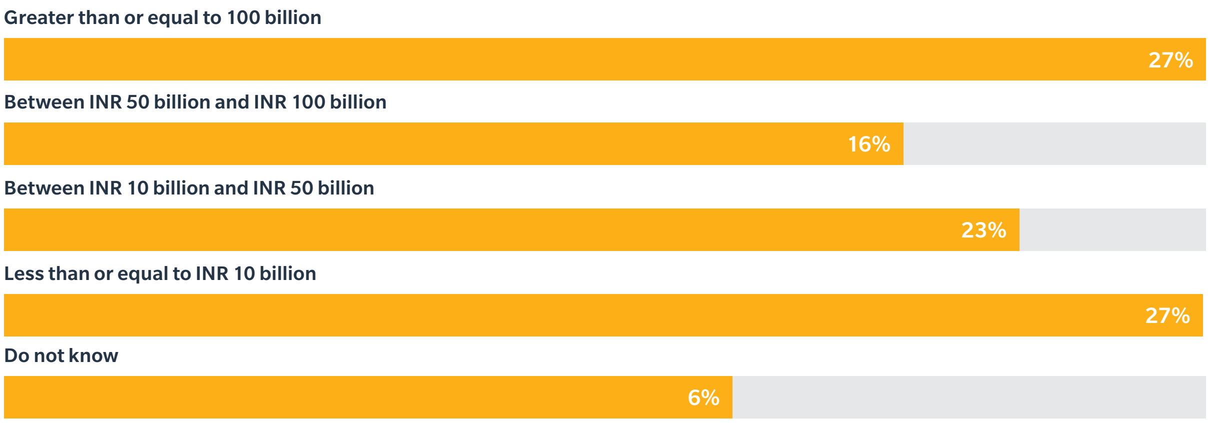


FIGURE 34

Where are you headquartered in India?

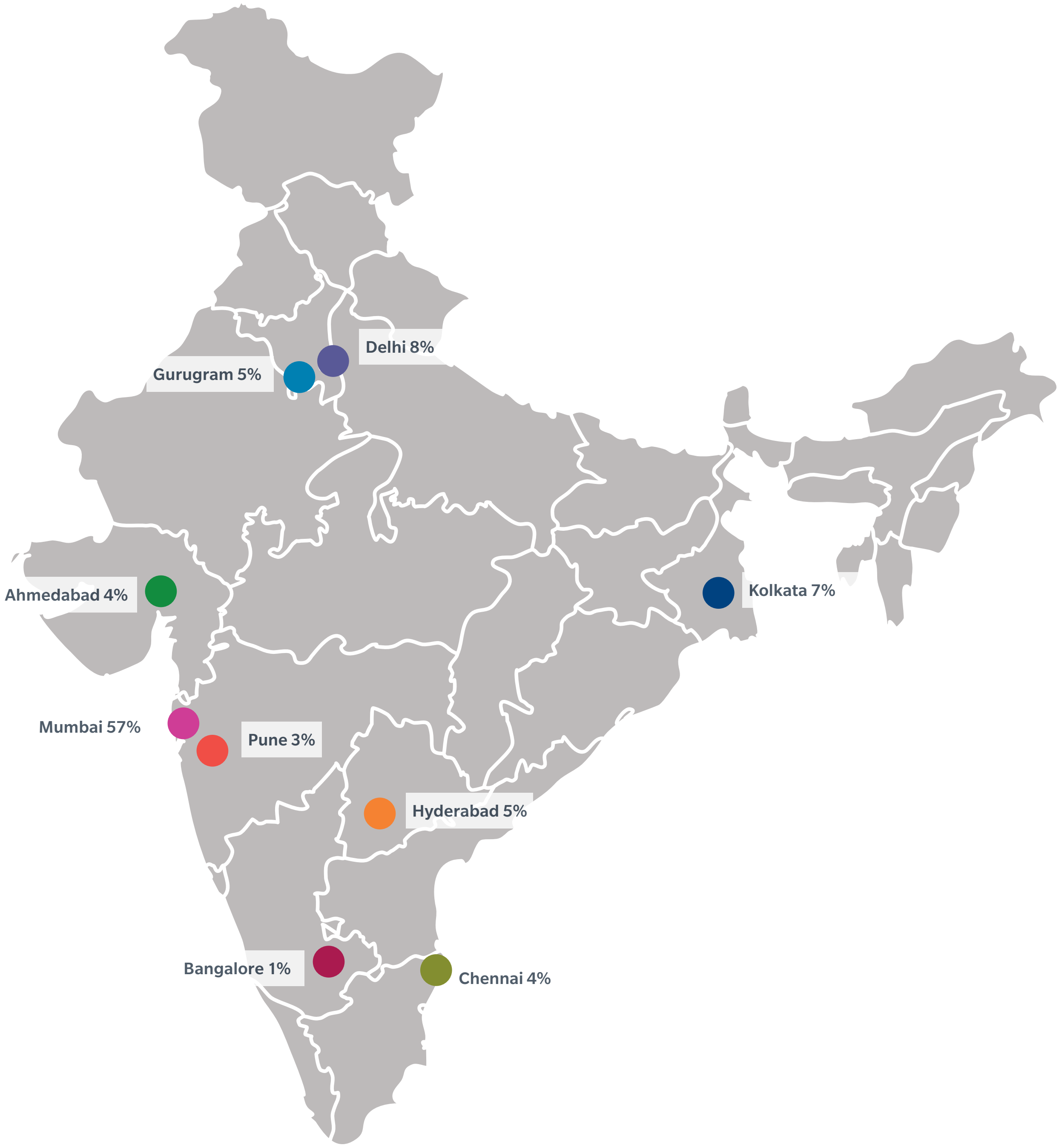


FIGURE 35

Please select the industry/sector that most closely matches that of your organization:

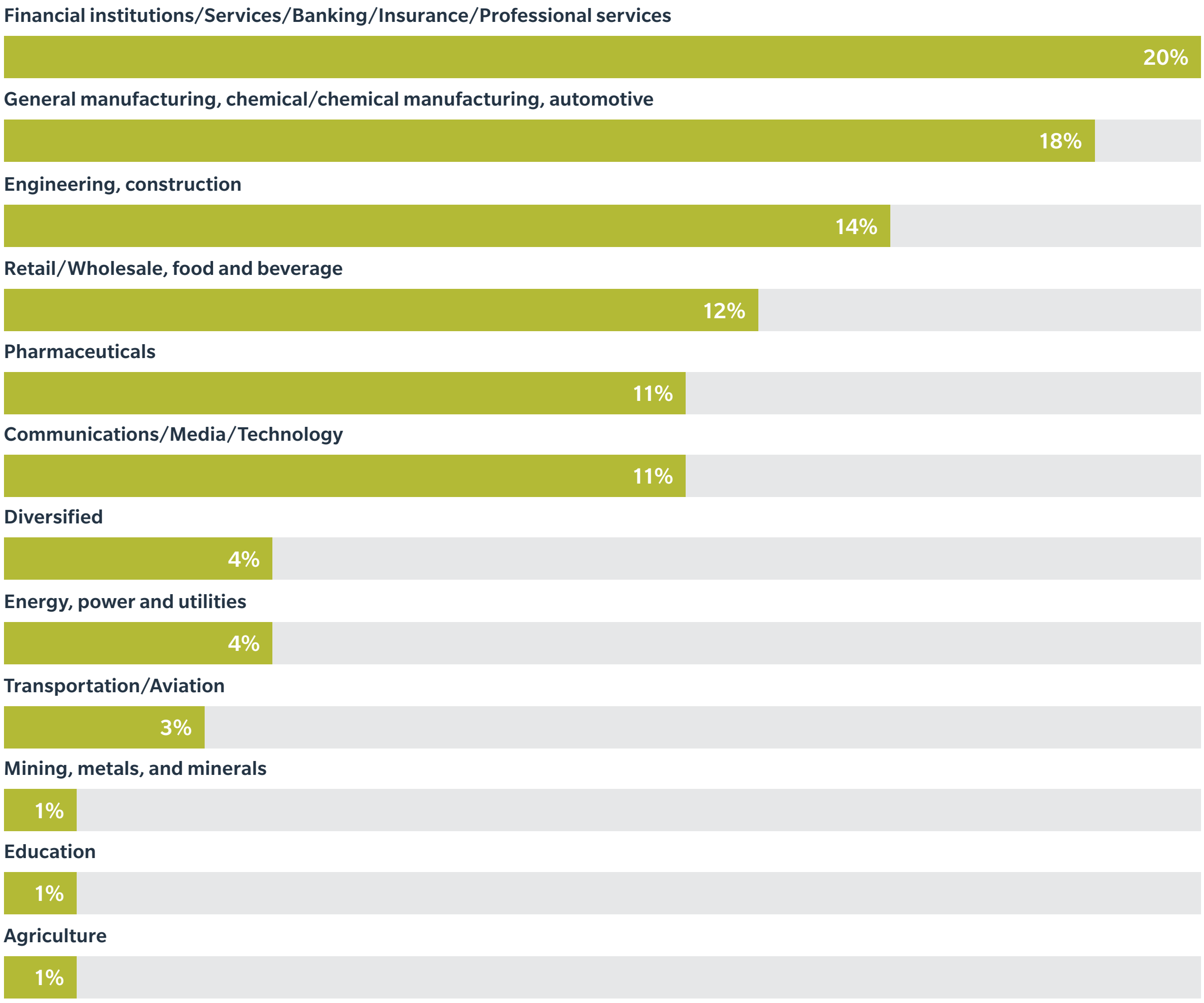


FIGURE 36

Your organization is a:

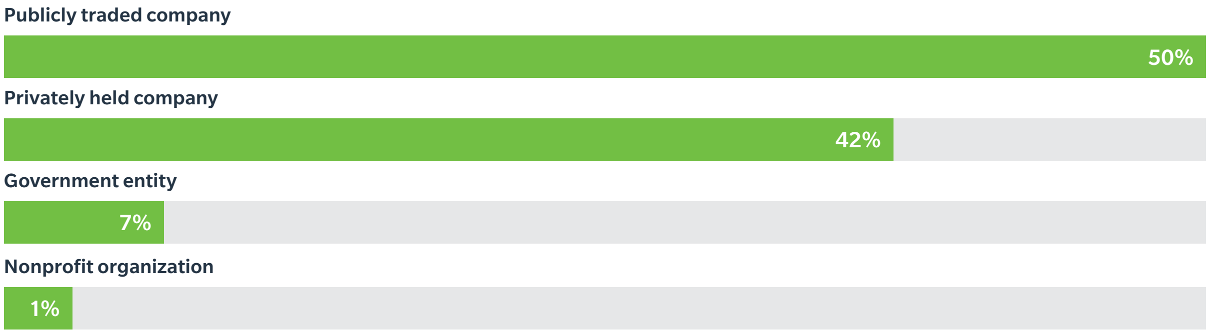
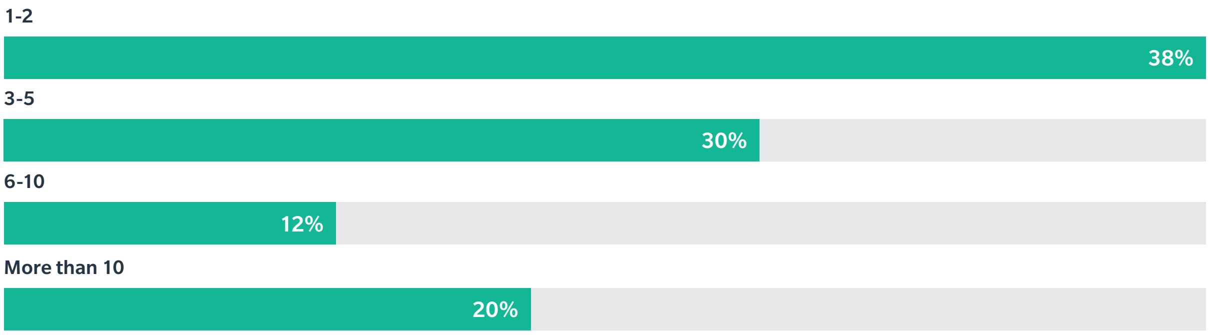


FIGURE 37

How many people are in your organization's risk management department?



Recent Publications

EXCELLENCE IN RISK MANAGEMENT XV

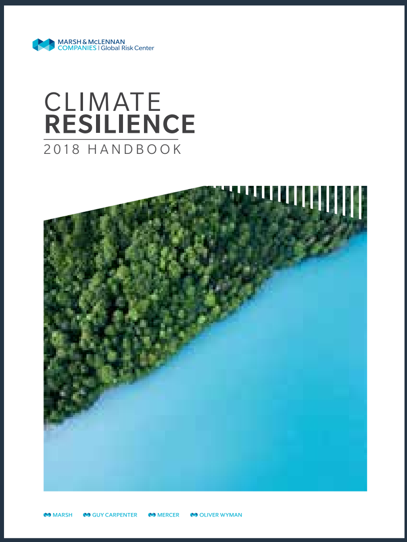
Technology is embedded in nearly every aspect of our lives, including in many businesses' critical functions and risk professionals are tasked with answering critical questions about the risks these new technologies present. A collaboration between Marsh and RIMS, this year's Excellence in Risk Management survey investigates risk professionals' views on their role in innovation as well as their companies' digital approach.

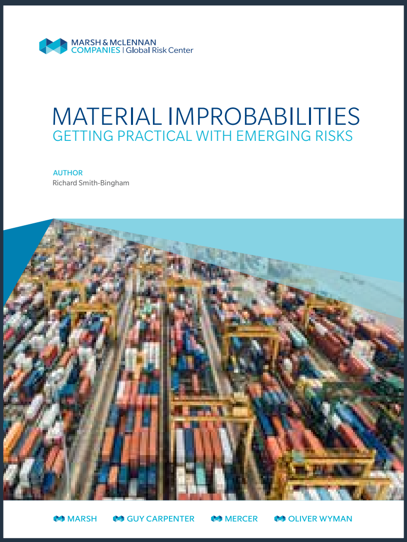
FROM THREATS TO IMPACT: EVOLVING RISK CONCERNS IN ASIA PACIFIC VOL. 3

Leveraging the 2018 Global Risk Report, the report builds on previous iterations by providing insights regarding the risk landscape for businesses operating in Asia-Pacific. It also drills down into the risks of critical infrastructure failure/ shortage and talent shortage, before exploring several options to mitigate such risks going forward.

CYBER EVOLUTION: EN ROUTE TO STRENGTHENING RESILIENCE IN APAC

A collaboration between FireEye and Marsh & McLennan Companies – each a leader in their own fields – the white paper includes a full overview of the fundamental cyber challenges facing the APAC region, and the appropriate risk management tools needed to address those challenges.





CLIMATE RESILIENCE 2018 HANDBOOK

The handbook provides concise cases that will change the way you think about climate in the context of your organization in three categories of action:

i. Strategies for Climate Resilience

ii. Financing for Climate Resilience

iii. Risk Management for Climate Resilience.

CYBER RISK MANAGEMENT RESPONSE AND RECOVERY

A collaboration between WomenCorporateDirectors and Marsh & McLennan Companies' Global Risk Center outlines everything directors need to know to position cyber insurance within a comprehensive risk management framework.

MATERIAL IMPROBABILITIES GETTING PRACTICAL WITH EMERGING RISKS

This publication from Global Risk Center sets out how firms can move from generalized concerns to analyses, discussions and actions in response to specific threats that may most disrupt their ambitions and operations and erode most value. It concludes by reflecting on the opportunities for Risk leaders to reframe the function to meet the needs of the new era.

Bibliography

1. Marsh & McLennan Companies Asia Pacific Risk Center. From Threats to Impact Evolving Risk Concerns in Asia-Pacific | Volume 3. (Marsh & McLennan Companies Asia Pacific Risk Center, 2018).

2. PTI. Cyber attack of mammoth scale: Over 22,000 Indian websites hacked between April 2017 - January 2018. The Financial Express (2018).

3. Tribune Investigation. Rs 500, 10 minutes, and you have access to billion Aadhaar details. The Tribune (2018).

4. World Energy Council & Oliver Wyman. World Energy Trilemma Index 2018. (World Energy Council, 2018).

5. ET EnergyWorld. India's petroleum import bill rose 9 per cent last fiscal, import dependency of crude rises to 82 percent. ET EnergyWorld (2017).

6. PTI. PM Modi tells oil producers high crude prices are hurting global growth. ET EnergyWorld (2018).

7. Hudson Lockett, Kate Beioley & Robin Wigglesworth. Oil prices extend their rise to a four-year high near $82. Financial Times (2018).

8. PTI. Germanwatch climate report on India not all encompassing: Government. The Economic Times (2018).

9. Lloyd's. A World at Risk Closing the insurance gap. (Lloyd's, 2018).

10. 10. Sushmita Choudhury Agarwal. Kerala floods: Insurers expect Rs 500 crore hit from claims. (2018).

11. State Planning Board, Thiruvananthapuram, Kerala, India. Economic Review 2017. (2018). Available at: http://spb.kerala.gov.in/ER2017/web_e/ch21.php?id=2&ch=21. (Accessed: 18th October 2018)

12. Santoli, M. Second-longest bull market ever aging gracefully, but investors wonder how long it will last. CNBC (2017).

13. Asit Ranjan Mishra. India tells US it won't accept caps on steel, aluminium exports. Livemint (2018).

14. Symantec. Internet Security Threat Report Volume 23. (Symantec, 2018).

15. Gemalto. Number of Breach Incidents by Source. Breach Level Index (2018). Available at: https://breachlevelindex.com. (Accessed: 17th October 2018)

16. Ponemon Institute & IBM Security. 2017 Cost of Data Breach Study. (Ponemon Institute, 2017).

17. Vindu Goel, Kai Schultz & Hari Kumar. Mumbai Shuts Down as Protests Erupt Over Caste Tensions. The New York Times (2018).

18. Telle, O. Emerging infectious diseases in India: the scourge that could boost urban development. The Conversation (2018).

19. Kakkar, M., Vong, S. & Sharma, A. Antibiotic resistance and its containment in India. BMJ (2017). doi:https://doi.org/10.1136/bmj.j2687

20. Hawthorne, J. The Water Crisis In India: Everything You Need To Know. Business Connect World (2018).

21. Luo, T. 40% of India's Thermal Power Plants Are in Water-Scarce Areas, Threatening Shutdowns. World Resources Institute (2018).

22. Marsh & RIMS. Excellence in Risk Management XIII Emerging Risks: Anticipating Threats and Opportunities Around the Corner. (Marsh, RIMS, 2016).

23. Smith-Bingham, R. The Emerging Risks Quandary Anticipating Threats Hidden in Plain Sight. (Marsh & McLennan Companies Global Risk Center, 2016).

24. Marsh & McLennan Companies Asia Pacific Risk Center & FireEye. Cyber Evolution En Route to Strengthening Resilience in Asia-Pacific. (Marsh & McLennan Companies Asia Pacific Risk Center, 2017).

25. Dylan Black, A. Kate Margolis, G. Benjamin Milam & Emily M. Ruzic. A Guide to Cyber Insurance. (the risk management societyTM, 2018).

26. Oliver Wyman. Taming Cyber Quantifying Cyber Risks Using a Structured Scenario Approach. (Oliver Wyman, 2018).

27. Reserve Bank of India. Risk Management Systems – Role of the Chief Risk Officer (CRO). (2017).

28. Balaji, S. India Finally Has A Data Privacy Framework -- What Does It Mean For Its Billion-Dollar Tech Industry? Forbes (2018). Available at: https://www.forbes.com/sites/sindhujabalaji/2018/08/03/india-finally-has-a-data-privacy-framework-what-does-it-mean-for-its-billion-dollar-tech-industry/. (Accessed: 24th October 2018)

29. Marsh & RIMS. Excellence in Risk Management XII Organisational Dynamics: A Focus for Effective Risk Management. (Marsh, RIMS, 2015).

30. Josh Salter. Exploring The Risk Committee Advantage. (the risk management societyTM, 2015).

31. Marsh & RIMS. Excellence in Risk Management XIV Ready or Not, Disruption is Here. (Marsh, RIMS, 2017).

32. Marsh Risk Consulting & RIMS. Reimagine Risk Capturing Opportunities in a World of Risk Navigating Uncertainty Third Risk Management Benchmark in Latin America. (Marsh Risk Consulting, RIMS, 2018).

33. Brandon P. Righi. Top Five Steps For Communicating With Executives. (the risk management societyTM, 2018).

34. Julie Cain, Christine Novotny & David J. Young. Communication with the C-Suite and Board. (the risk management societyTM, 2018).

35. the risk management societyTM. Strategic & Enterprise Risk Center - What is ERM? the risk management societyTM (2018). Available at: https://www.rims.org/resources/ERM/Pages/WhatisERM.aspx. (Accessed: 28th October 2018)

36. Oliver Wyman. Achieving Greater Value Through Risk Management. (Oliver Wyman, 2014).

37. Mark Farrell & Dr. Ronan Gallagher. Testing Value Creation Through ERM Maturity. (the risk management societyTM, 2015).

38. the risk management societyTM. Strategic & Enterprise Risk Center - RIMS Risk Maturity Model. the risk management societyTM (2018). Available at: https://www.rims.org/resources/ERM/Pages/RiskMaturityModel.aspx. (Accessed: 28th October 2018)

39. NACD. Adaptive Governance: Board Oversight of Disruptive Risks. (NACD, 2018).

40. Marsh & McLennan Companies Global Risk Center & Women Corporate Directors. Cyber Risk Management Response and Recovery Global Governance Insights in Emerging Risks. (Marsh & McLennan Companies Global Risk Center, 2018).

41. Marsh. Marsh Expands IBM Collaboration to Provide Blockchain Proof of Insurance to More Clients Through Salesforce Platform. Marsh (2018). Available at: https://www.marsh.com/us/media/marsh-expands-ibm-collaboration-to-provide-blockchain-proof-of-i.html. (Accessed: 20th October 2018)

42. English, E. Can Blockchain Help Reduce the Financial Industry's Cyber Risk? BRINK (2018).

43. Why a universal technology platform is key to addressing India's banking woes. Moneycontrol (2018).

44. Rebello, J. New RBI unit to track blockchain and AI. The Economic Times (2018).

45. Marsh. North American Retail/Wholesale Roundtable Succeeding in the Retail Revolution. (Marsh, 2018).

46. Hawkins, S. Fintech sandboxes in Asia-Pacific region. Asia Business Law Journal (2018).

47. The Economic Times. RBI to form regulatory sandbox for fintech, set up data science lab. The Economic Times (2018).

48. Marsh & RIMS. Excellence in Risk Management XV Maintaining Relevance Amid Technology Disruption. (Marsh, RIMS, 2018).

ABOUT MARSH

A global leader in insurance broking and innovative risk management solutions, Marsh's 30,000 colleagues advise individual and commercial clients of all sizes in over 130 countries. Marsh is a wholly-owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With annual revenue of over US$14 billion and nearly 65,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading firms. In addition to Marsh, MMC is the parent company of Guy Carpenter, Mercer, and Oliver Wyman. Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube; or subscribe to our free news service BRINK Asia.

ABOUT MARSH INDIA

Marsh India Insurance Brokers Pvt Ltd is a joint venture between Marsh International Holdings Inc. and its Indian partners. It started its operations in 2003 and is the first foreign broker to get composite broking license by the IRDAI. Currently, with presence in 15 branches across the country, with over 600 employees and local market understanding backed by international expertise and global networks, it provides risk and insurance advisory to more than 4,000 clients in India. Follow Marsh India on LinkedIn.

ABOUT MARSH & MCLENNAN COMPANIES' ASIA PACIFIC RISK CENTER

Marsh & McLennan Companies' Asia Pacific Risk Center addresses the major threats facing industries, governments, and societies in the Asia-Pacific region, and serves as the regional hub for our Global Risk Center. Our research staff in Singapore draws on the resources of Marsh, Guy Carpenter, Mercer, Oliver Wyman, and leading independent research partners around the world. We gather leaders from different sectors around critical challenges to stimulate new thinking and solutions vital to Asian markets. Our digital news service, BRINK Asia, keeps decision makers current on developing risk issues in the region. For more information, visit www.mmc.com/asia-pacific-risk-center.html or email the team at contactaprc@mmc.com.

ABOUT RIMS

RIMS, the society for risk management™, is a non-profit organization that represents more than 3,500 companies, government organizations, and NGOs around the world. Dedicated to the development of risk management for the success of organizations, RIMS offers networking, professional development, and educational opportunities for its members: more than 10,000 risk managers in more than 60 countries. For more information visit: www.rims.org.

In India, RIMS has been working with local risk practitioners since 2017 to engage, educate and advocate for Indian Risk Management professionals. The Society seeks to build an engaged community of risk professionals committed to sharing ideas, networking, and advancing the practice of risk management.

ABOUT THIS REPORT

This report is based on 123 responses to an online survey with C-suite executives and risk professionals from leading firms across 19 industries conducted by Marsh and RIMS in September 2018, along with expert input from MMC and RIMS.

We hope that in coming years, with the growing membership base of RIMS and the Marsh client base, we can further expand and deepen the findings of this survey.