Marsh | RIMS the risk management society

Excellence in Risk Management India

Advancing towards resilience

December 2021

“ **Organisations cannot afford to be complacent. They must continue to scan the horizon for emerging risks and proactively support the development of solutions that fuel resiliency and sustained growth.**

Contents

Foreword

From natural catastrophes to cyberattacks to a global public health crisis, organisations around the world, and in India, had to manage significant risks in the past two years. Existing risks evolved and new risks emerged. Rapid changes forced organisations to quickly adapt business models and processes, and shift strategies.

Organisations that embraced risk-aware cultures were better prepared to navigate this perfect storm of risk. However, this experience reinforced the importance of a strong risk and insurance function as a part of the organisation's strategy. Organisations cannot afford to be complacent. They must continue to scan the horizon for emerging risks and proactively support the development of solutions that fuel resiliency and sustained growth.

In the 4th edition of the *Excellence in Risk Management India* report, *Advancing towards resilience*, Marsh and RIMS, *the* risk management society®, explore how the fallout from the COVID-19 global pandemic continued to concern organisations. But, beyond health and safety concerns, business interruption, new remote work settings, and a greater reliance on technology — and the cybersecurity issues that stem from that reliance — have prompted organisations to re-evaluate their exposures, and equally as important, their mitigation and risk financing strategies.

Business leaders across India continue to demonstrate their deep appreciation for the power of risk management to not only address the adverse effects of uncertainty, but to support innovation and growth opportunities. With that appreciation comes greater expectations. RIMS and Marsh are proud to be able to deliver this insight to support risk professionals as they meet and exceed their organisations' strategic objectives.

On behalf of Marsh and RIMS, we would like to thank all of the risk professionals who contributed to the survey. We continue to work together towards advancing the risk management profession in India and across the globe.

Sincerely,

Sanjay Kedia
Country Head & CEO
Marsh India

Ellen Dunkin,
RIMS 2021 President

Introduction

The second and subsequent waves of the COVID-19 pandemic brought to the fore the fragility of health systems and the complexity of risks in interconnected businesses. It shifted the risk landscape of organisations across geographies and industry segments, and highlighted the importance of resilience. The *Excellence in Risk Management India* report delves into Indian corporates' perception of their future key risks and their preparedness for them.

Cyber risk remained one of the key risks on the horizon for organisations, likely due to the sustained shift in work patterns and a large number of employees continuing to work from home.

The COVID-19 pandemic had a far-reaching impact on both organisations and individuals, which could also be seen in people risks becoming an important component of organisations' preparedness. Indian corporates actively took steps to safeguard employee health and well-being as a part of their effort to retain talent.

While the risk management function in India continues to evolve, companies are taking preliminary steps towards developing resilience through risk monitoring, acknowledging the need for increased risk awareness, and investing in integrating risk management within their strategic planning.

Indian companies are at an important juncture. Their ability to manage emerging risks will determine their ability to survive and thrive.

Marsh and RIMS, *the* risk management society®, hope that this year's *Excellence in Risk Management India* report, *Advancing towards resilience*, will help you understand the current landscape and promote discussion of risk management within your organisation.

We encourage you to reach out to us with any questions or comments.

Health, economic, and cyber concerns high on risk radars

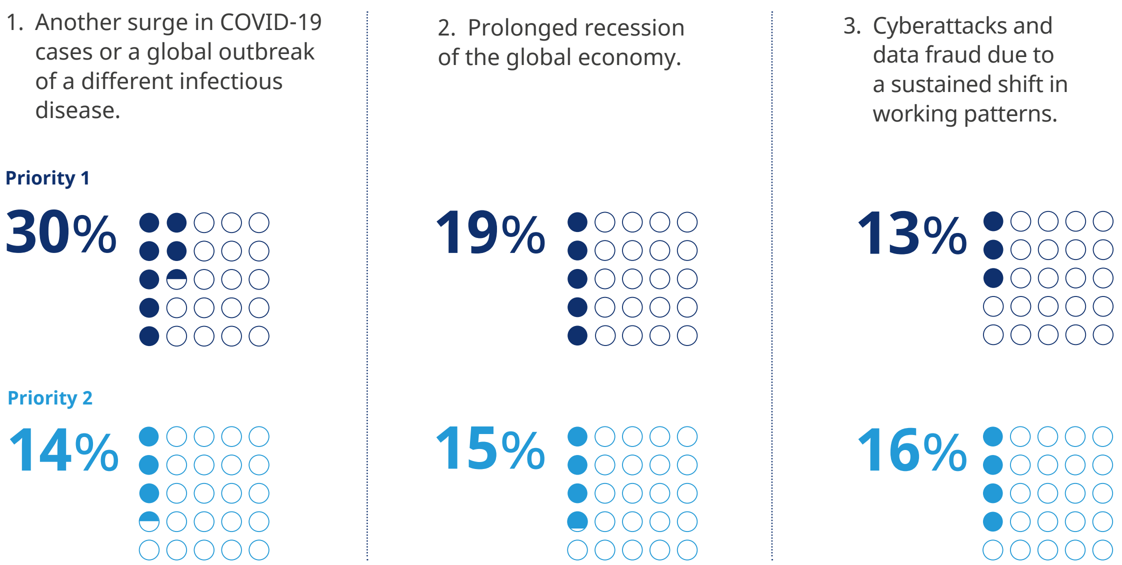
For the second consecutive year, the continued effects of the COVID-19 pandemic and concerns about a future public health crisis were top-of-mind for Indian business leaders, according to the 2021 *Excellence in Risk Management India* survey. Close to a third of survey respondents said another surge in COVID-19 cases or another infectious disease outbreak was the most impactful short-term risk facing their organisation (see Figure 1).

Respondents viewed a prolonged recession as the number two short-term risk, followed by cyberattacks and data fraud. It's worth noting that both economic worries and cyber risks are generally seen as being heightened by the pandemic.

The COVID-19 pandemic continued spreading around the world in 2021, even as vaccines started to become available. In India, daily confirmed cases, as well as deaths, peaked in May 2021, straining the country's healthcare system and economy.

01 | Impact of infectious diseases remains the top concern?

Q: Which short-term risks do you expect to affect your company post-pandemic? Rank according to priority level.



“Indian organisations remain concerned about the potential of a prolonged global recession.

According to the Organisation for Economic Co-operation and Development (OECD), India’s economy contracted by close to 8% in 2020, while the world’s economy contracted by 3.5%. Despite the OECD’s projections for economic expansion — both in India and globally — in 2021 and 2022, the potential for a prolonged global recession remains a concern for organisations in India.

The shift to a remote workforce necessitated by sweeping lockdowns to stem the spread of the pandemic is widely seen as having increased cyber risk. The Indian Computer Emergency Response Team (CERT-In) data indicated that cyberattacks in India rose by 300% in 2020, according to news reports. And cyber risk remained elevated in 2021, with more than 600,000 cybersecurity incidents reported in the first six months of the year alone, according to CERT.

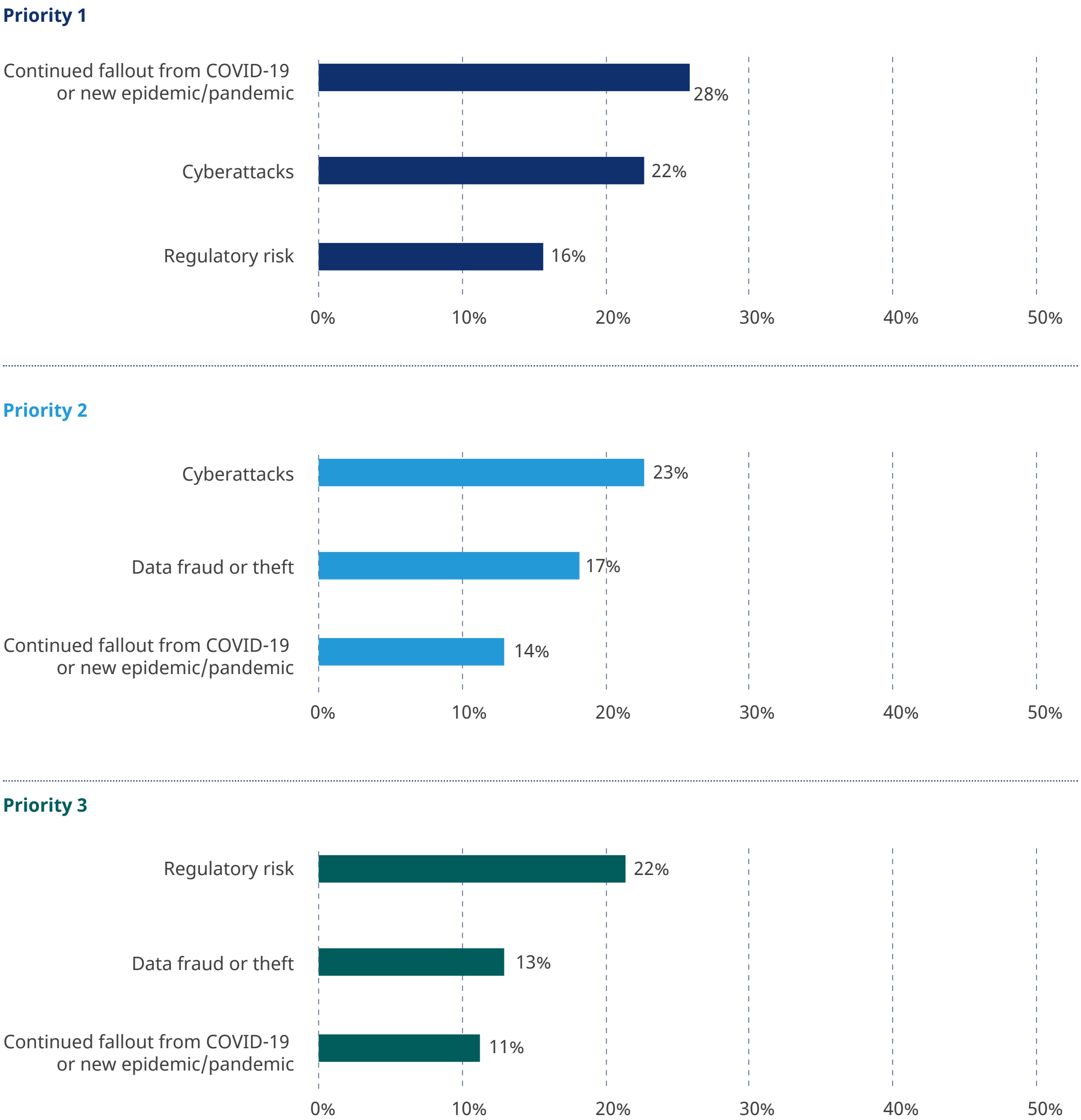
Aside from causing millions of deaths around the world — more than 5 million at the time of writing — the pandemic disrupted supply chains, stretched healthcare resources, required drastic changes in work practices, and more.

> “The COVID-19 pandemic underscores the fragility of global economies faced with a fast-spreading infectious disease.

The pandemic has had extensive and long-lasting impacts on organisations across the globe. It is understandable that many survey respondents saw a continued fallout from COVID-19 or other public health crises as not just their top short-term risk, but also their top long-term one (see Figure 2).

02 | COVID-19, cyber risks worry Indian business leaders

Q: Where will the next long-term critical risks for your organisation emerge from? Rank according to priority level.



Pandemic highlights the need for resilience

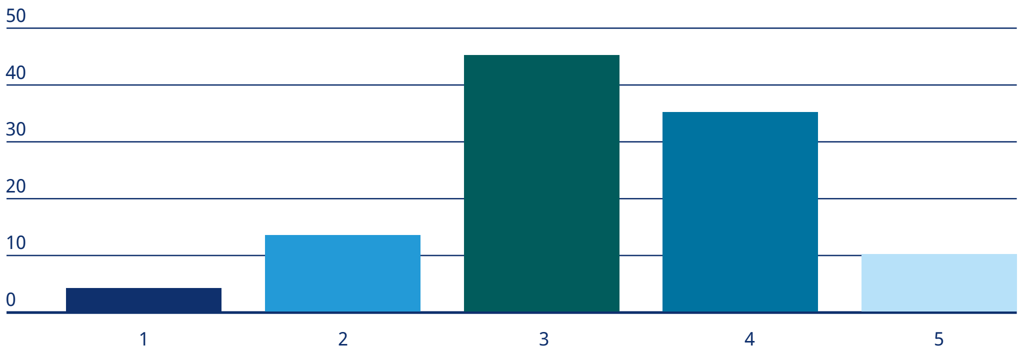
The pandemic has shifted the risk landscape of organisations across geographies and industry segments. And it has underscored the importance of having robust risk management practices that go beyond ticking compliance boxes.

Perhaps because they are still managing the effects of COVID-19, survey respondents gave overall low marks for organisational preparedness for the pandemic or a similar communicable disease outbreak. Only 10% of survey respondents said they are fully prepared for the continued fallout from COVID-19 or a new epidemic/pandemic (see Figure 3).

This raises the question: What does preparedness mean for Indian organisations? For many, risk preparedness simply relates to their ability to respond to insurers' queries, allowing organisations to recoup losses suffered.

03 | Despite high concern, few feel prepared for infectious disease risks

Q: Rate your preparedness for a continued fallout from COVID-19 or a new epidemic/pandemic. Use a scale of 1 to 5, with 1 being "not prepared" and 5 being "fully prepared".



But advanced companies use robust risk management strategies to prepare for both current and emerging risks, in other words, to become more resilient. Marsh has identified four common behaviours among companies that are on the path to becoming more resilient: anticipating risk; connecting risk management to business strategy; avoiding the gaps in the perception of preparedness; and measuring relevant data.

- **Anticipation:** Resilient companies expect the unexpected. They have crisis management plans in place, but they also dig deeper, look farther ahead. Consider that during the pandemic even organisations with thorough business continuity plans struggled. Why? Many of them didn't fully anticipate the widespread, long-lasting damage a pandemic could create.
- **Integration:** Another key behaviour among resilient organisations is to fully integrate risk management with operations and strategy. Doing so increases the ability to develop effective responses. Most organisations do not connect resilience planning with their long-term investment strategy. Those that do make the connection are on the path to better mitigating financial exposure, reputational damage, business interruption, and other losses.
- **Preparedness:** On the journey to resilience, it's important to develop an accurate perception of an organisation's preparedness. A false sense of security can halt an organisation in its tracks. Companies often overestimate how quickly and effectively they will be able to respond to and recover from a given risk.
- **Measurement:** There is no shortage of data and analytics in today's business environment. But consistently applying metrics can be a stumbling block. Many companies fail to conduct a high rate of modeling and forecasting even on risks they see as important. And among the companies that do so, most only model in select areas.

The past two years have shown the toll that a low frequency event can take on organisations, and the difficult recovery faced by those that are not sufficiently prepared. As interdependencies — economic and otherwise — increase, the risk landscape becomes increasingly complex. Organisations need to be prepared not only for high-frequency risks, but also for those that are less likely, but may be significantly more impactful.

COMPANIES LOOKING FOR EFFECTIVE INSURANCE COVERAGE

Achieving the right level of risk transfer is an important aspect of preparedness. However, half of *Excellence India* survey respondents said that available insurance does not cover all of their organisation's critical emerging needs (see Figure 4).

04 | Half of companies say insurance does not meet all emerging risk needs

Q: Please finish the following sentence by selecting one of the options below: "The insurance coverage for critical emerging risks available in today's market..."

37%

Meets all of my organisation's needs.

50%

Meets some of my organisation's needs, but does not cover all critical emerging risks.

3%

Does not need my organisation's needs.

Despite the high potential losses associated with emerging risks, many Indian organisations are still struggling to secure sufficient coverage. Lack of reinsurance support for new products has negatively affected innovation in coverage for many emerging risks; this has led to a lack of available insurance solutions while available ones may be priced prohibitively high.

Until they are able to secure sufficient coverage, Indian corporates are keenly looking at risk management strategies that help them better manage their most pressing risks. But the right risk management plans will remain effective even after risk transfer solutions are available and can even help organisations secure needed coverage and terms and conditions.

“Cybersecurity preparedness is never complete. The residual risk always remains.

CISO at a Mumbai-based bank.

2

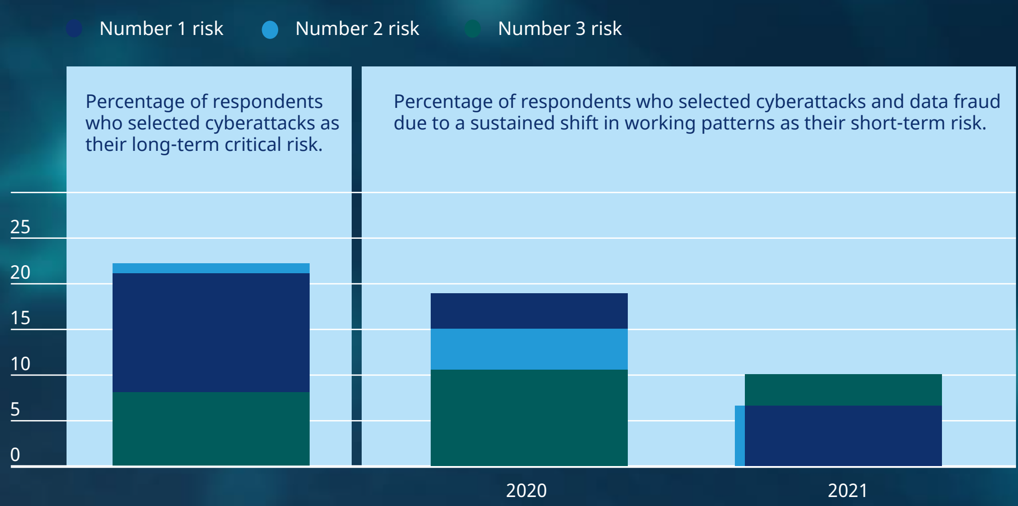
Cyber risks remain high priority for Indian organisations

The shift at many companies to remote work during the pandemic, combined with ongoing digitisation, opened new doors for cyber criminals. Indian government data shows that in 2020 alone there were more than 1.1 million cyberattacks.

Against this backdrop, it is not surprising that cyber risk remains a major concern for Indian companies, and is considered among the top three short-term and long-term risks (see Figure 5).

05 | Cyber risk remains a major concern

Q: Where will the next long-term critical risks for your organisation emerge from?



Note that in the second year of the pandemic, concern around cyberattacks intensified due to a change in working patterns and lack of information. Many employers in India are looking at transitioning to a more flexible working system. Some extent of remote work is expected to remain, leading to concerns of increased cyberattacks due to unsecured home networks. Yet, less than a quarter of *Excellence India* survey respondents said they were fully prepared for a cyberattack in either the near- or long-term.

Information theft is considered the biggest threat to Indian corporates, with more than a quarter of *Excellence India* survey respondents listing this as their top concern (see Figure 6). This concern may be due to a number of publicised data thefts and leaks taking place in 2021, including the leaking of personal data of an airline's passengers and records of a fast food outlet's customers.

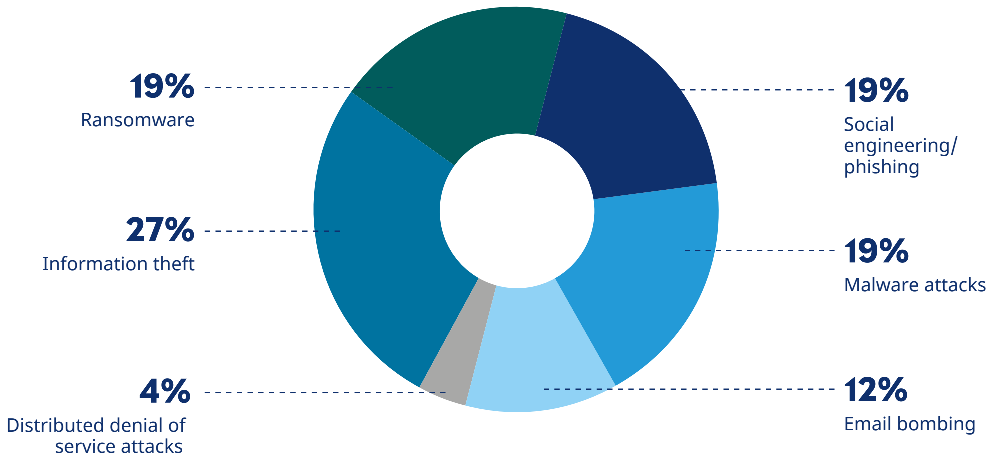
Other types of cyber incidents, including ransomware, are also of concern for Indian companies. It is believed that by the end of this year, global businesses will be the target of ransomware every 11 seconds, up from every 14 seconds two years ago. Costs, downtime, and remediation efforts to recover from a ransomware attack are also rising.

Cyber incidents could lead to long-term effects for organisations. Survey respondents noted that reputational damage or an effect on clients/customers would be the most damaging to their organisations.

Indian companies are taking action to improve their overall cyber resilience, with close to half of *Excellence India* survey respondents saying their top priority is investment in updating cybersecurity tools and processes. A fifth of respondents are focusing on employee training and education, and are leaning on risk transfer solutions to protect themselves and become more resilient.

06 | Information theft is the biggest cyber threat for survey respondents

Q: In the current cyber environment, which among the following is the most threatening to your organisation?



TIGHTENING UP YOUR IT ENTERPRISE: 12 KEY CYBER HYGIENE CONTROLS

By implementing cyber hygiene controls, starting with the first five, organisations can improve their cybersecurity posture and resilience.

Multifactor authentication for remote access and admin/privileged controls.

Email filtering and web security.

Secured, encrypted, and tested backups.

Privileged access management (PAM).

Endpoint detection and response (EDR).

Patch management and vulnerability management.

Cyber incident response planning and testing.

Cybersecurity awareness training and phishing testing.

Hardening techniques, including remote desktop protocol (RDP) mitigation.

Logging and monitoring/ network protections.

End-of-life systems replaced or protected.

Vendor/digital supply chain risk management.

As they seek to improve their cyber resilience, companies should make sure they have the correct cyber hygiene controls in place, focusing especially on:

- Increased security through multifactor authentication (MFA). Requiring at least two pieces of evidence to confirm a user's identity can provide a substantial barrier to entry for hackers.
- Endpoint detection and response software. This widely available software gathers critical information about a device used by an employee and watches for any suspicious or irregular activities.
- Secure and encrypted backups that are regularly tested. Backups may help organisations recover faster following a cyber incident and are especially important considering increased ransomware activity. Backups need to be encrypted and updated at regular intervals.
- Privileged access management systems and their proper use. Organisations should require the use of higher security login credentials to access administrator or privileged accounts.
- Email filtering and web security systems to reduce instances of malicious content. These systems seek to identify any messages that include links or attachment, and thoroughly screen any flagged attachments.

It's not sufficient to establish cybersecurity controls; companies need to apply extreme diligence in maintaining them. And controls are only one important step in an organisation's cybersecurity posture. Organisations need to have systems in place that allow them to quickly identify and effectively respond to a potential attack.

As the chief information security officer of a Mumbai-based bank noted, cybersecurity preparedness is never complete and residual risk will always remain. Thus, the protection offered by cyber insurance is critical for recovery following a potential attack.

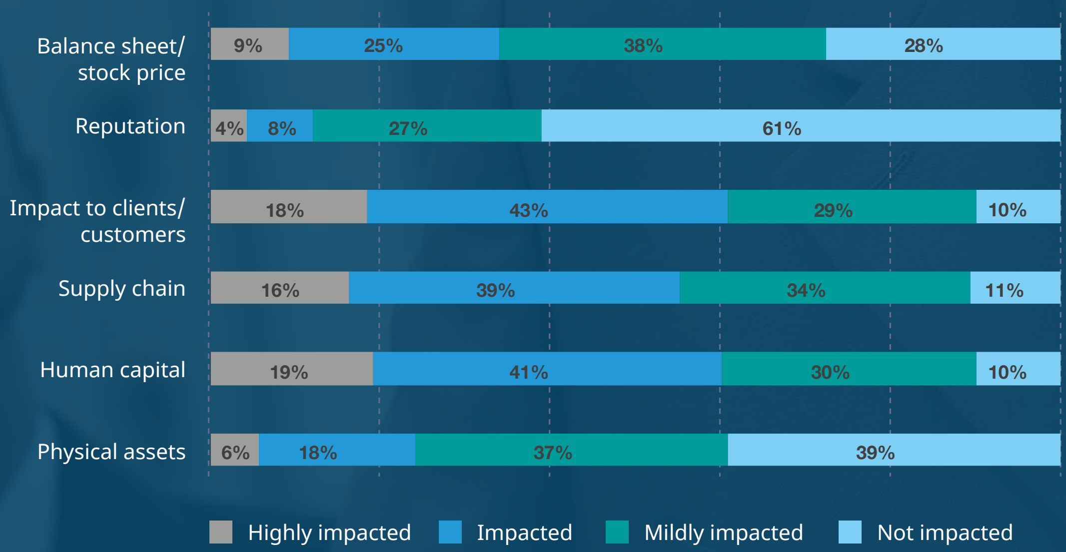
Pandemic impact on employees ranks high

The ripples of COVID-19 have permeated all core business areas — and the impact on people risk should not be overlooked. Survey respondents rated the pandemic's effect on human capital to be as significant as its impact on clients and customers, and greater than on such areas as reputation and balance sheet/stock price (see Figure 7).

Respondents said that the areas of talent attraction, retention, and engagement are most likely to affect their businesses (see Figure 8).

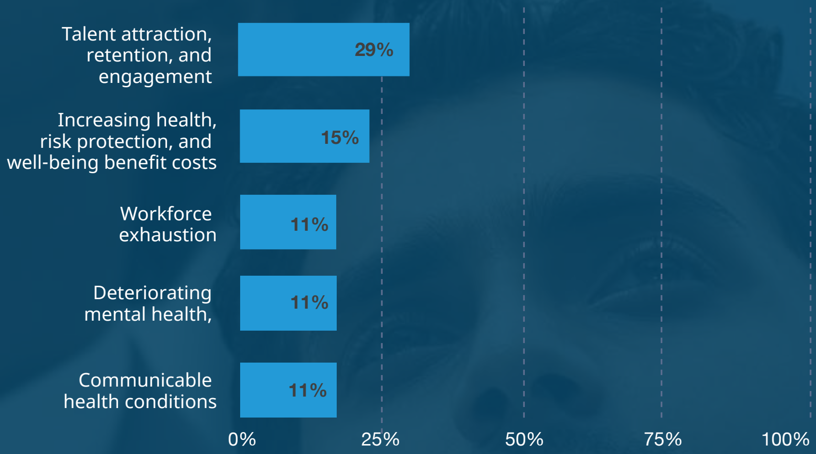
07 | **Human capital most affected by pandemic**

Q: Please rate the impact the pandemic has had on the following core business areas.



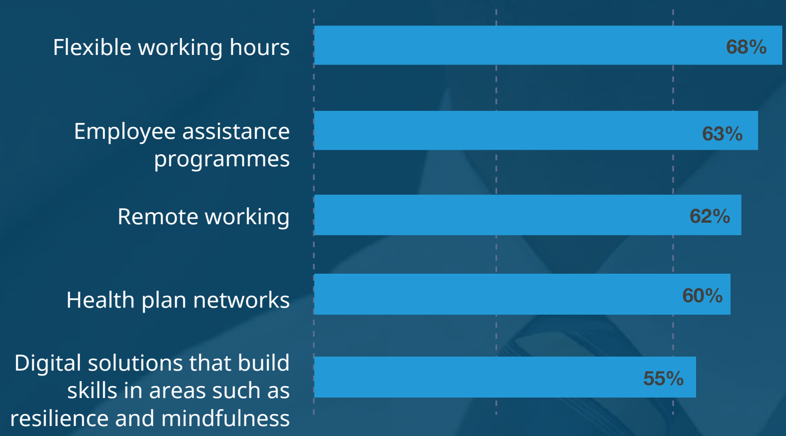
08 | Talent issues among companies' top concerns

Q: Which one of the below people risks do you deem most likely to impact your business?



09 | Flexible and remote working among top three employee support actions

Q: Which of the following measures is your organisation taking to support employee mental/emotional well-being? Select all that apply.



Respondents were also concerned about increasing costs of health, risk protection, and benefits, ranking this as the second-most likely people risk to affect business. Cost containment can be challenging, and when not managed properly can have a significant impact on a business's bottom line.

An effective incident prevention and intervention programme is essential for managing people risk, as is having a robust approach to incident cause identification. However, in the midst of the pandemic, and with an increase in working from home, these programmes may be tested and lines blurred. It is paramount that these programmes are revisited by businesses in India to ensure they are fit for purpose in the current business environment.

An area of workforce health gaining global attention is mental well-being. Roughly two-thirds of respondents said that their organisations were using flexible working hours and remote working as ways to support employees' mental well-being, which can be challenged during times of crisis (see Figure 9).

However, the isolation of working from home — alongside fears relating to the pandemic and potential loss of income — can trigger or exacerbate mental health issues. Training regarding mental health and well-being can help managers and supervisors to develop more effective strategies to support their workforce and maintain productivity.

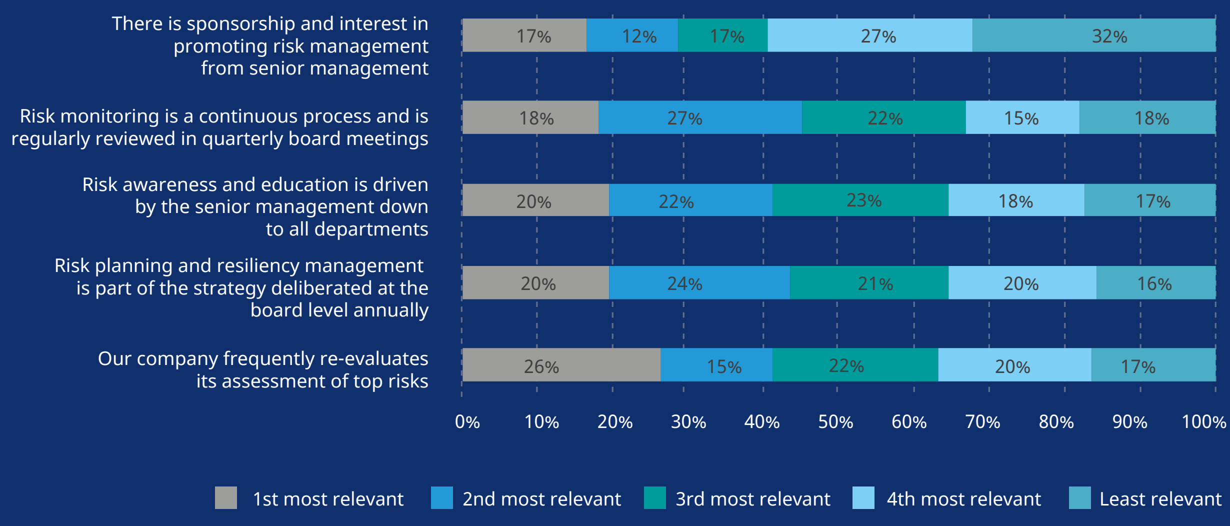
Risk management Current and future state

The practice of risk management continues to evolve in companies in India, with many seeking to optimise this element of business strategy. For example, a significant segment of respondents frequently re-evaluate their assessment of top risks, with over 25% making this a top priority (see Figure 10).

Risk monitoring was also recognised as a key continuous process that respondents regularly review in their quarterly board meetings.

10 | Quarter of companies frequently re-evaluate top risks assessment

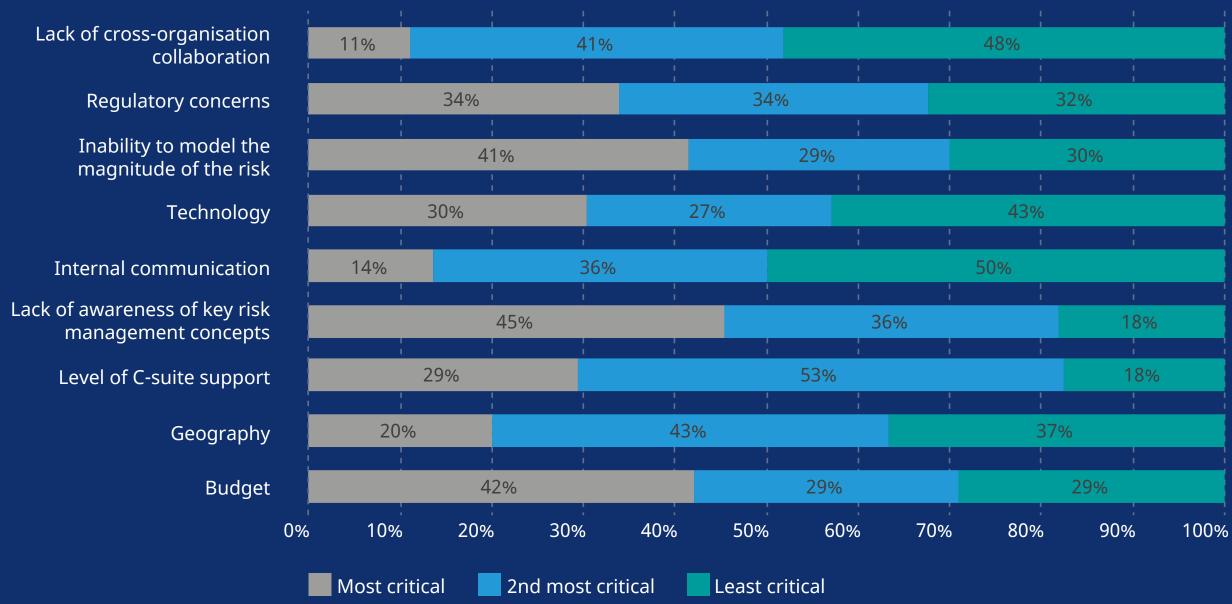
Q: Rank the below statements in order of their relevance for your organisation, with #1 being most relevant and #5 being least relevant.



Budget was cited by 42% of respondents as the most critical barrier to understanding the impact of emerging risks on risk management, (see Figure 11). Still, more than half (55%) intend to increase investment in risk management (see Figure 12).

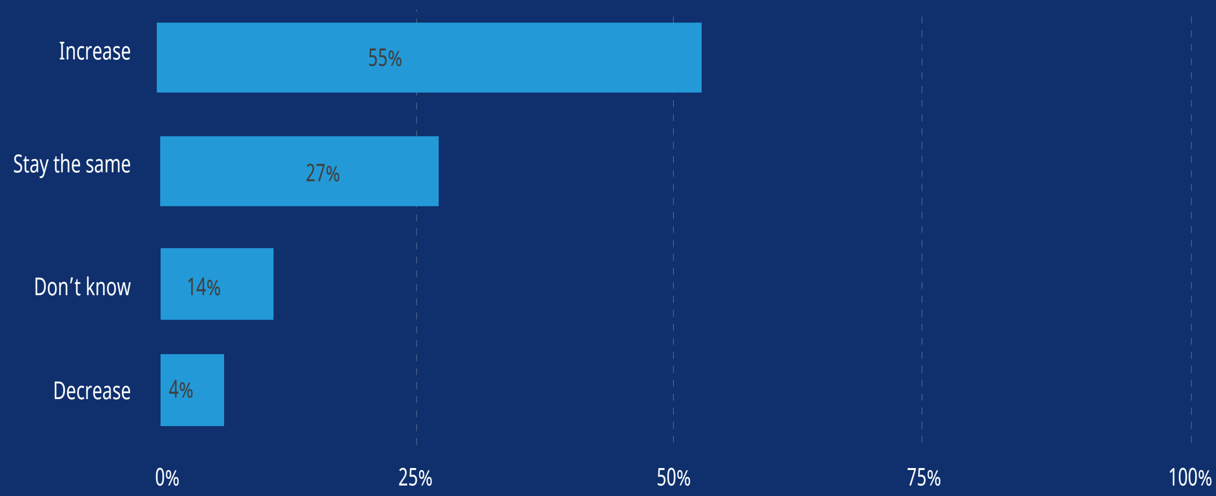
11 | Awareness, budget, and risk modelling most likely to hinder understanding effect of emerging risks

Q: What barriers inhibit your organisation's ability to understand the potential impact of emerging risks on business strategy and risk management decisions? Choose three and rank them in order of criticality, with #1 being the most critical barrier.



12 | Majority increasing risk management investment

Q: In 2022, our organisation's investment in risk management will:



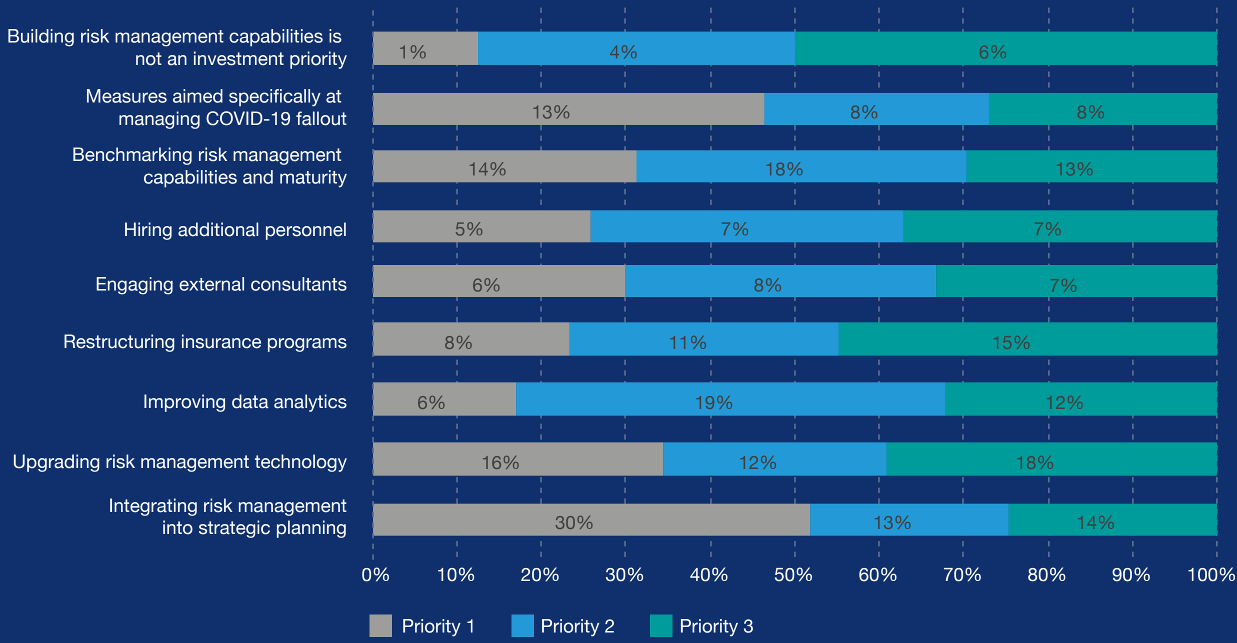
The number one risk management investment priority for respondents in 2022 will be integrating risk management into strategic planning. Key to this will be using risk modelling, which ranked as the third most critical barrier to understanding the impact of emerging risks (see Figure 13).

Such approaches can be expected to help businesses manage crises similar to COVID-19, but will need to be modified for considering other critical risks, such as extreme weather, climate change challenges, and cyber risks. Focusing on resilience will help to develop transferable skills, processes, and techniques, and build a more strategic response to risk.

While work continues to overcome these barriers and develop risk management strategies, 65% of respondents use lessons learned — presumably from their response to COVID-19 — to enhance their agility and strategic positioning. Other approaches include modifying day-to-day processes within the organisation (61%) and implementing digitally enabled work processes and backup solutions (55%) (see Figure 14).

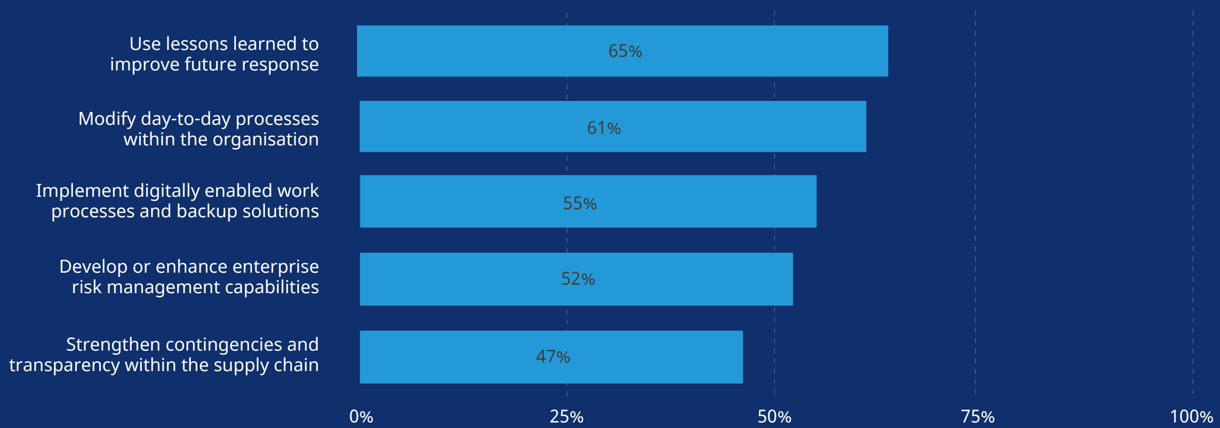
13 | Risk management integration tops list of 2022 investment priorities

Q: Which of the following risk management areas will be your top investment priorities in 2022?



14 | Companies using lessons from past experiences to improve future responses

Q: Which of the following risk approaches is your company using or planning to use to enhance its agility and strategic positioning?



Key takeaways

- For organisations in India, the COVID-19 pandemic continues to heighten both economic worries and cyber risks.
- The shift to remote working during lockdowns is widely seen as having increased cyber risk, with reports of more than 600,000 cybersecurity incidents in the second half of 2021.
- Organisations in India need a deeper understanding of risk preparedness to build resilience against future critical events.
- To build resilience, organisations should embed the four best-practice behaviours identified by Marsh — anticipating risk; connecting risk management to business strategy; avoiding the gaps in the perception of preparedness; and measuring relevant data.
- Achieving the right level of insurance is paramount to preparedness; where organisations are unable to secure sufficient coverage for critical emerging needs, solid risk management strategies are essential.
- The practice of risk management continues to evolve within organisations in India, and many intend to increase investment in their risk management as they seek to optimise this element of business strategy.

RECOMMENDATIONS

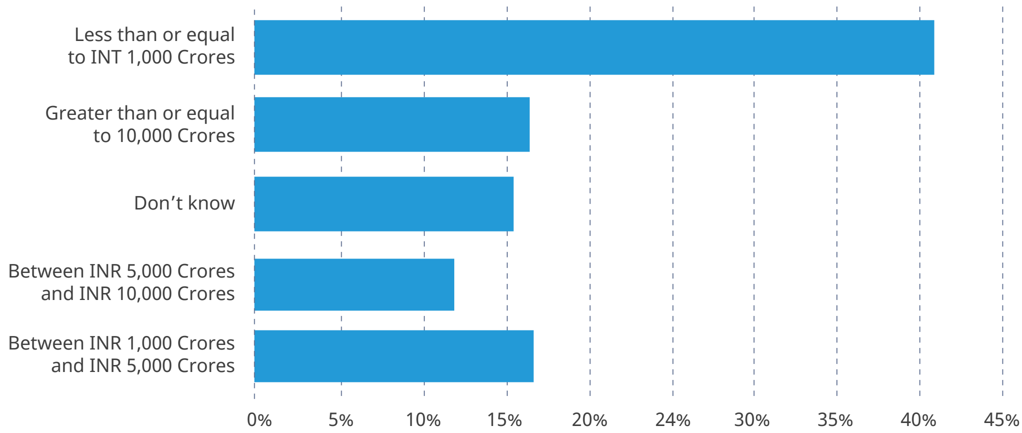
Focus on resilience: Resilience means being able to absorb the impact from a range of emerging risks and depends in large part on having robust risk management strategies in place. This includes anticipating risk, connecting risk management to business strategy, ensuring your organisation's perception of preparedness doesn't lead to a false sense of security, and measuring relevant data.

Invest in preparedness: Look beyond pandemic as you develop a risk management strategy that is prepared to respond to any number of emerging risks. For example, shifting work patterns have intensified an already escalating cyber risk landscape that calls for a range of responses, from scenario planning to financial quantification.

Apply COVID-19 lessons: The COVID-19 pandemic brought to light a number of weaknesses in organisations' preparations for health care crises. Companies should prepare to manage the ongoing impact from the current pandemic as well as the potential for another major infectious disease event.

Survey demographics

15 | Organisation size, by revenue



RESPONDENT INDUSTRIES (TOP 5)

- Financial Institutions/ Services/Banking/Insurance
- Pharmaceuticals
- Automotive
- General Manufacturing
- Construction

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 40,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue over $18 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit mmc.com, follow us on LinkedIn and Twitter or subscribe to BRINK.

About RIMS

RIMS, the risk management society®, is a global not-for-profit committed to advancing the practice of risk management throughout the world. RIMS brings networking, professional development, certification, and education opportunities to our membership of 10,000 risk management professionals in over 60 countries. Founded in 1950, the Society represents more than 3,500 industrial, service, nonprofit, charitable, and government entities throughout the world. To access RIMS Risk Knowledge resource library and for additional information about the Society, visit www.RIMS.org.