MARSH | RIMS the risk management society

EXCELLENCE IN RISK MANAGEMENT | NOVEMBER 2019

State of Risk Management in India 2019

MARSH & McLENNAN COMPANIES

EXCELLENCE IN RISK MANAGEMENT | NOVEMBER 2019

State of Risk Management in India 2019

CONTENTS

Foreword

In today's global business environment, organisations have myriad opportunities to explore and enter new international markets.

Technology enables most globalisation efforts, and paves the way for global success by enhancing communications, improving processes, and connecting businesses as they collaborate and embrace opportunities. As highlighted in the second annual *Excellence in Risk Management India* report from Marsh and RIMS, the risk management society®, we can see that innovation and technology come with significant risk. It's no surprise, then, that information security is top of mind for business leaders in India and around the world.

Whether a firm's priority is to protect critical data from cyber-attacks or to manage the impact of other top issues such as extreme weather events, corporate culture is paramount to navigating the world's evolving risks.

Enterprise risk management (ERM) is integral to establishing a risk-aware corporate culture. As more organisations recognise the link between a formalised ERM programme and better performance, risk professionals must seize the opportunity to develop advanced capabilities.

At the same time, expectations of risk management are growing. Effective risk professionals are now much more than commercial insurance buyers. They are educators, communicators, and strategic thinkers who are ready to address emerging and short-term risks while helping to plan a company's long-term goals.

Marsh and RIMS invite the country's thriving risk management community to engage with our risk management resources. We invite you to tap into our vast collections of risk management knowledge and experience, which have allowed thousands to become their organisations' champions for innovation, growth, and revenue-generating initiatives.

Sincerely,

SANJAY KEDIA
Country Head & CEO
Marsh India

GLORIA BROSIUS
RIMS-CRMP
RIMS 2019 President

Whether a firm's priority is to protect critical data from cyber-attacks or to manage the impact of other top issues, corporate culture is paramount to navigating the world's evolving risks.

More companies recognise the importance of implementing a comprehensive risk management framework.

Introduction

Risk management in India is at a turning point, faced with an increasingly global, digital, and interconnected business environment in which threats and vulnerabilities evolve quickly.

To meet the challenges, risk managers are seeking to expand their knowledge base, hone their skillsets, and access best practices, tools, and technologies.

At the same time, the *Excellence in Risk Management India 2019* survey shows that traditional cybersecurity strategies and investments continue to lag, despite a clear need for more effective risk management in the country. The good news is that more companies recognise the importance of implementing a comprehensive risk management framework to improve their ability to manage risk and turn it into a competitive advantage.

The survey sheds light on the need to strengthen the risk management function and instill it throughout the organisation. It also emphasises building risk resilience to cope with emerging risks from an end-to-end risk management perspective.

This year's survey focused on the top risks facing Indian corporates, including the dominance of cyber and data security risks, risk management priorities and challenges, and key insurance solutions for emerging risks.

The responsibilities of risk management teams now often extend into leading risk governance and compliance and actively influencing strategic growth decisions by addressing new and emerging risks.

This year's survey respondents highlighted the 'implementation of a formalised enterprise risk management (ERM) programme' as the biggest performance gap in their organisations' risk management functions. We also found a clear disconnect between strategic decision-making related to risk management at the C-suite level and the realities of company-wide implementation felt by risk departments.

This disconnect between strategy and implementation mirrors the performance gaps relating to ERM implementation and education of employees whose role does not generally involve risk management. Such gaps were felt most acutely by the risk management teams on the ground.

Marsh and RIMS, the risk management society®, hope you find this year's *Excellence in Risk Management – State of Risk Management in India* report useful for promoting discussion of risk management in your organisation.

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

Cyber and Weather Events Viewed as Top Risks in India

Cyber-attacks are the highest priority for most companies

For the second consecutive year, respondents to the survey ranked cyber-attacks as the number one critical risk facing their organisations, with extreme weather events a distant second (see Figure 1). More than half of organisations deemed cyber-attacks as their number one priority, nearly four times the number prioritising weather events.

It's interesting to note both the similarities and contrasts with other risk surveys conducted at a global level.

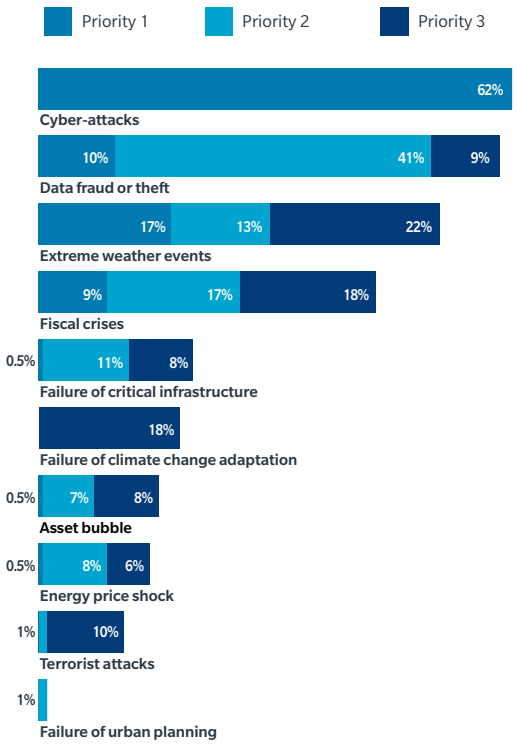
The World Economic Forum's recent *Regional Risks for Doing Business 2019* report placed cyber-attacks as the second highest risk concern globally, behind fiscal crises.

With the region facing a number of risks related to climate change – from more frequent and higher intensity storms to drought and water crises – it was not surprising to see weather events as a high priority. This is underscored in the *Regional Risks for Doing Business 2019*, where business leaders placed water crises as their top risk in South Asia.

FIGURE 1

Cyber-attacks top the risk priority list for Indian companies.

Q: Amongst the following areas, where do you think the next critical risks for your organisation will emerge from? (Choose three and rank them in order of criticality.)



Nearly 70% of respondents said their organisation had felt no impact or only minor impact from a cyber event in the past 24 months.

Cyber Threats Evolve, Companies Say Impacts Vary

Organisations May Be Underestimating Their Vulnerability

The number of cyber-attacks continues to increase globally. In India alone, more than 394 million data records have been lost or stolen in publicly disclosed breaches between 2013 and 2018, according to the Gemalto Breach Level Index and Varonis. That would equal about 4% of the 9.7 billion data records lost globally during that time. Indeed, India was the second most affected country when it came to targeted cyber-attacks between 2016 and 2018, according to *Symantec's Internet Security Threat Report*.

Globally, the repercussions of cyber-attacks often extend beyond financial losses and the loss of confidential data. Cybersecurity breaches may also trigger other issues, such as business interruption losses. These threats are further amplified through the increasing use of the Internet of Things (IoT) and similar technologies that rely on interconnectivity between devices to bring greater convenience.

Furthermore, the interconnectivity of control systems in critical infrastructure can lead to an accumulation of risks, which may lead to unforeseen events from a cyber-attack. For example, the failure of a power grid or telecommunications network due to a cyber event can impact numerous businesses. A cyber event can also threaten vendors and other third parties.

Still, many survey respondents feel that their company has yet to be greatly affected by a cyber event (see Figure 2). Nearly 70% of respondents said their organisation had felt no impact or only minor impact from a cyber event in the past 24 months.

FIGURE 2

Cyber-attacks top the list of Indian risk management concerns.

Q: How have you been affected by cyber-attacks (including denial of service, intrusion, malware, ransomware, and data leakage) in the last 24 months?

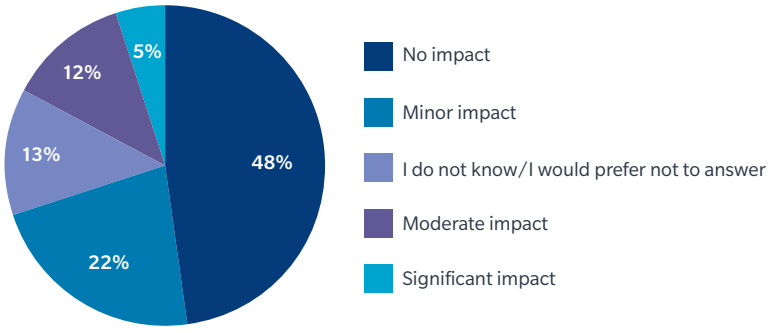
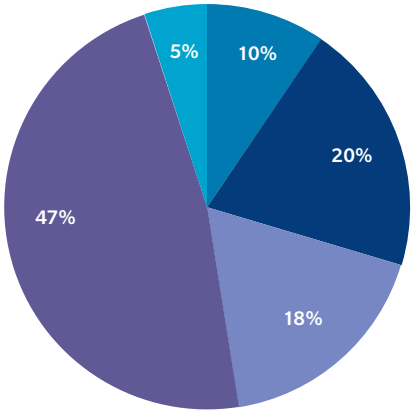


FIGURE 3

Nearly half of companies say they have the highest level of data security.

Q: How mature is your data security (including areas such as at-rest encryption, in-transit encryption, information leakage prevention, integrity monitoring)?



- Data protection policies have been defined and communicated to the relevant staff, but compliance is not mandatory.
- I do not know/No opinion.
- Policies have been defined, communicated, and the necessary technical controls have been implemented, but they are not reviewed regularly.
- Policies have been defined, communicated, and the necessary technical controls have been implemented. We also have online monitoring processes to prevent information leakage and periodic reviews of policy compliance.
- We do not have any data protection policies.

Given the pervasiveness of cyber-attacks, the numbers appear to minimise the damage likely felt by organisations. It's possible that some respondents are unaware of cyber events that have occurred at their companies, perhaps a reflection of the often-siloed responsibility for managing what are seen as IT risks. Others may be reluctant to acknowledge an event, based on a perceived stigma with admitting to cyber-attacks and the potential for reputational damage.

It can be challenging to accurately assess the impact of a cyber-attack when there are no large financial losses resulting from an isolated incident. In cases where financial losses have been recovered, companies may overlook other aspects of cyber-attacks that are difficult to recognise and even harder to quantify.

Still, more than half of respondents acknowledged some level of impact or said they didn't know or preferred not to say. And the rising digitalisation of businesses in India – due to the adoption of technologies related to cloud computing, mobile devices, social media, and the IoT – will only further expand the threat surface. Consider, for example, the recent increase in ransomware and malware attacks, which have broadened beyond larger firms and now cut across size ranges. According to Malwarebytes' *Cybercrime Tactics and Techniques Q1 2019* report, which reviews the firm's breach detections, ransomware detections for businesses increased 195% between the first and fourth quarters of 2018. India had the fourth largest case of detections at 7%, behind the US (47%), Indonesia (9%), and Brazil (8%).

Getting ahead of cyber threats is paramount. In 2018, the average cost for a data breach in India rose to INR 11.9 Cr (US$1.7 million), according to an IBM-Ponemon Institute study. This is an increase of 7.9% from 2017, with the average cost per record being INR 4,552 (US$64).

The growing awareness of the need and demand for more effective data protection and cybersecurity can be seen in the pending India Personal Data Protection Bill, being drafted along the lines of the EU General Data Protection Regulation (GDPR). Among other things, the law would establish a Data Protection Authority charged, in part, with overseeing the cross-border transfer of personal data. Timing of the legislation is uncertain at the time of writing.

Another growing concern globally is that cyber-attacks increasingly threaten critical infrastructure and, in turn, national security, thus prompting countries to strengthen their screening of cross-border partnerships. In the *2019 Global Cyber Risk Perception Survey*, conducted by Marsh and Microsoft, the majority of respondents said they were highly concerned about the potential impact of nation-state cyber-attacks.

Building Effective Cybersecurity

Among survey respondents, 47% said their organisations have a high level of data security that includes defined and communicated policies, technical controls, and online monitoring processes to prevent information leakage (see Figure 3). It's likely this includes a significant number who are expressing an inflated sense of their preparedness, which can create additional issues.

Even if taken at face value, that leaves more than half of respondents identifying as having less than the highest security measures in place or not knowing whether they have adequate data security.

Cyber-attacks increasingly threaten critical infrastructure and, in turn, national security.

India, like other countries, has been susceptible to malicious cyber-attacks and fallen prey to lax cybersecurity protocols. Ultimately, in order to capitalise on technology-based opportunities, digital literacy and competency within organisations needs to keep pace with the evolution of cyber threats.

As noted in the *2019 Cyber Perceptions Survey*, many organisations build a cyber risk management strategy based on prevention and investments in technological frontline cyber defenses (see Figure 4). Spending is often more limited for other cyber risk management resources, including cyber insurance or event-response training. Many organisations likely believe they can eliminate or manage cyber risk largely through technology, rather than by using a range of measures around planning, transfer, and response.

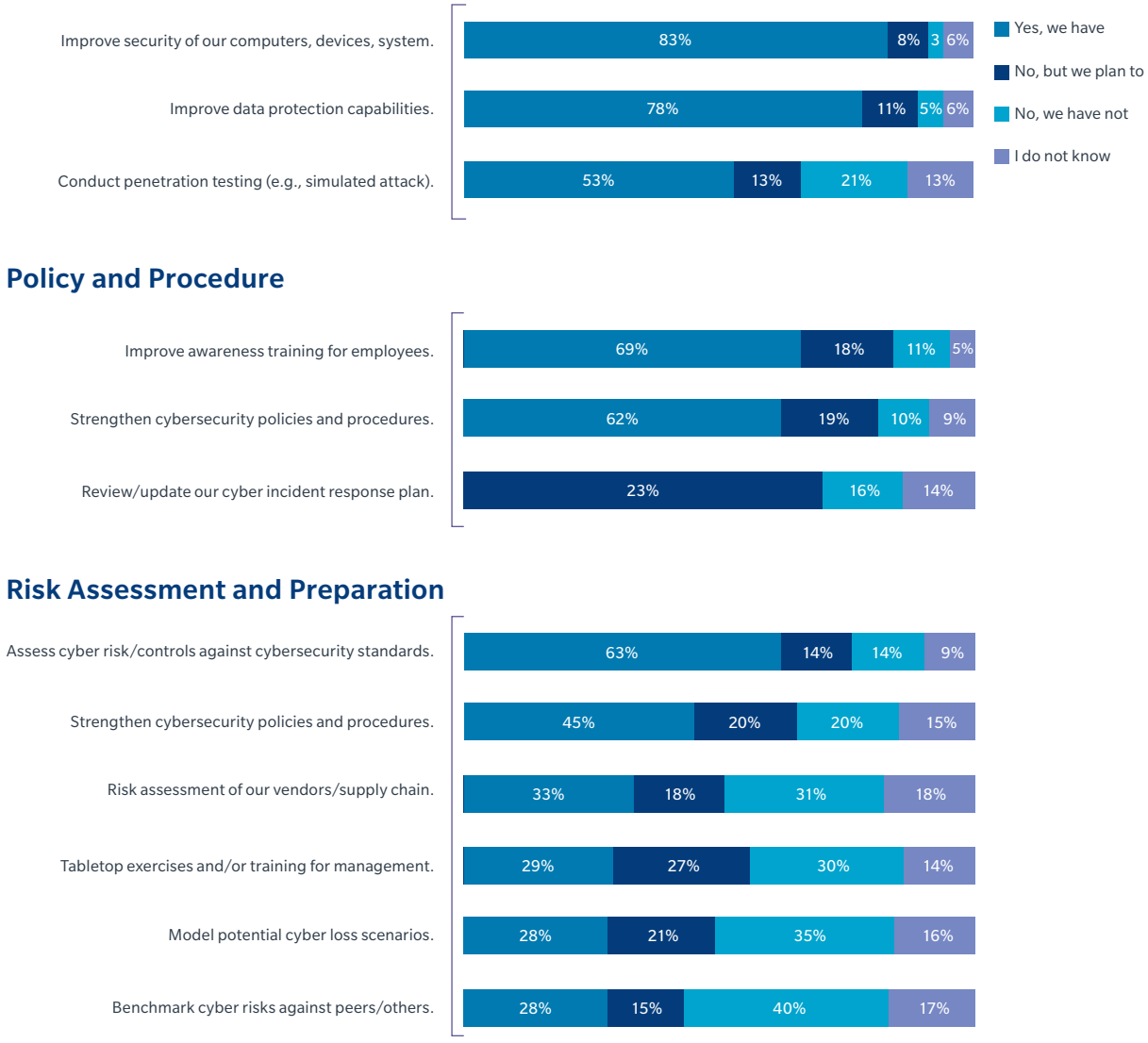
"Best practice calls not for parity of spending, but an investment strategy that, reflecting an organisation's unique risk profile and appetite, leverages the complementary roles of technology and insurance to deter cyber-attacks where possible and transfer the risk of those that cannot be prevented," the report states. "However, the emphasis on cybersecurity spending and technology over other measures reveals that many organisations have not yet embraced this truth."

FIGURE 4

Cyber risk actions tend to focus on technical measures.

Q: Please indicate whether your organisation has taken the specific actions listed below within the past 12 to 24 months.

SOURCE: MARSH MICROSOFT 2019 CYBER PERCEPTIONS SURVEY



Quantifying Cyber Risk

Though cyber-attacks top the list of emerging critical risks for organisations, it's nevertheless difficult for risk managers and others to highlight the potential damage in a way that all stakeholders can understand. And the cost of cyber events is only going to rise.

Quantifying cyber risk is thus an effective way to illustrate the potentially catastrophic effect that attacks or other cyber events can have on a company's bottom line.

Many businesses use simple qualitative terms – "high," "medium," or "low" – to describe their cyber risk. A more accurate monetary valuation can be provided by cyber risk quantification, which allows organisations to view cyber risk as they do other business risks. Aside from depicting a more detailed picture, it allows for better evaluation of cyber risk management investments and strategies.

Quantifying cyber risk can help your organisation make better informed capital allocation decisions, enable performance measurement, and frame cyber risk in the same economic terms as it does other enterprise risks.

Aligning Risk Management With Strategy

Investing in Strategic Risk Management Is Top Spending Priority

The survey found an overwhelming desire from respondents to make a stronger connection between risk management and strategic planning for the business. About two-thirds of respondents said that integrating risk management into strategic planning was their top investment priority for 2020 (see Figure 5).

Having that linkage to strategy can elevate the profile of a risk management department, giving it the often elusive "seat at the table" when making decisions about an organisation's overall approach to managing risk.

In an era in which most decisions are backed by data, it's notable that respondents' next two investment priorities were 'upgrading risk management technology' and 'improving data analytics'. Risk managers who are able to show data-driven reasoning behind their recommendations are more likely to be effective partners across the business and sought out by other departments. At the same time, investing in more efficient technology can help automate some risk management tasks, potentially freeing time for risk managers to pursue more strategic issues. While discussions are clearly being held at a senior strategic level, there is a discrepancy between organisations' risk management ambitions and capabilities on the ground.

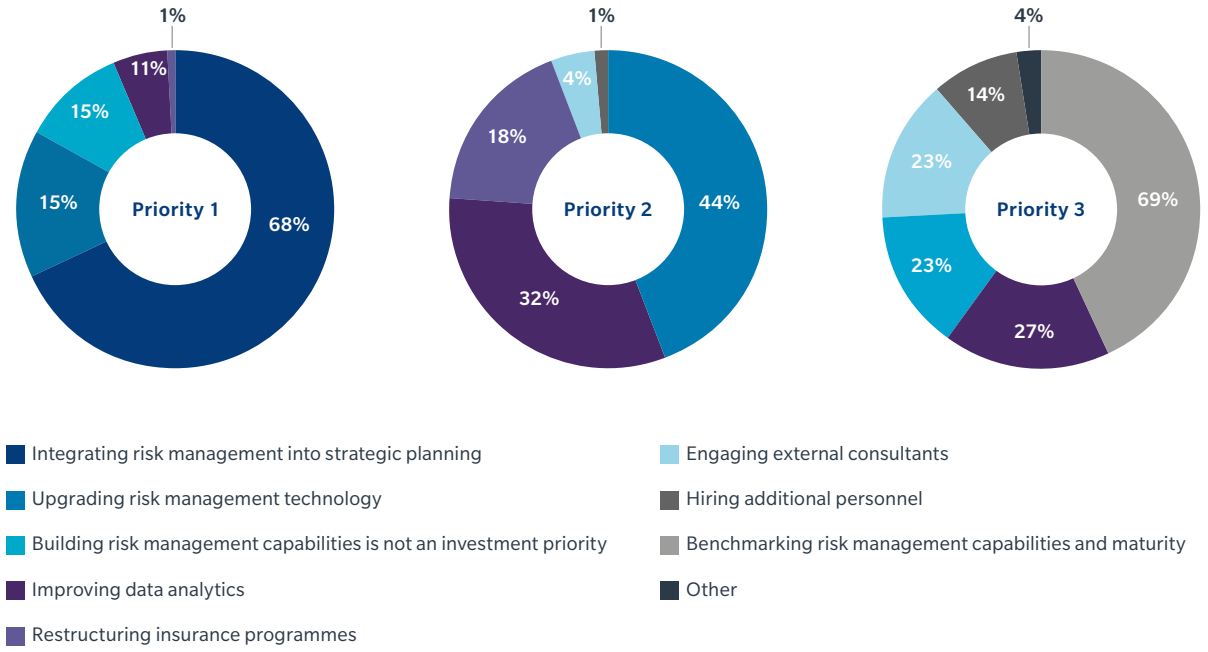
Respondents highlighted the 'implementation of a formalised enterprise risk management (ERM) programme' as the biggest performance gap in their organisations' risk management functions. Most respondents ranked 'educating other (non-risk) employees on key risk management practices' as the second performance gap. This call for education is a nod to the need for risk management capabilities to be generalised throughout organisations.

But finding the funds to upgrade technology and analytics capabilities is not always easy. For example, 'budget' was the number one barrier respondents said was inhibiting their organisation's ability to understand the impact of emerging risks on business strategy.

FIGURE 5

Organisations are seeking a more strategic role for risk management.

Q: Which of the following risk management areas are your top investment priorities for 2020?



Formal ERM Programmes Lacking

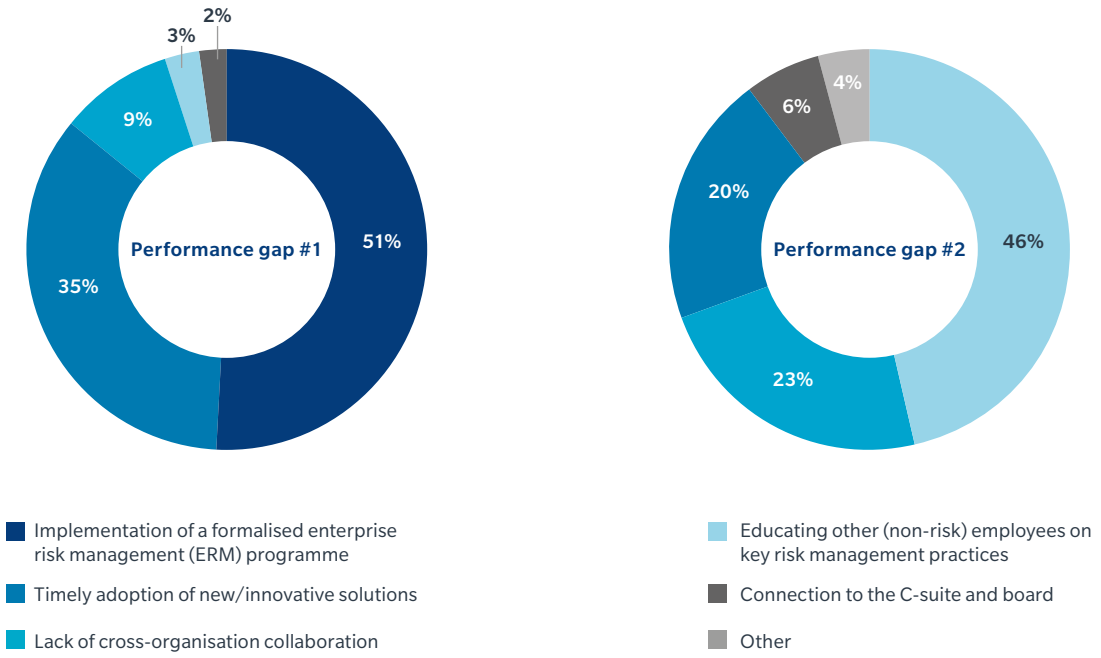
Globally, ERM programmes – sometimes referenced at more advanced stages as strategic risk programmes – have taken hold and become the norm in many regions. Survey respondents, however, said the lack of a formalised ERM programmes was the biggest performance gap in their organisations' risk management functions (see Figure 6).

In what can be viewed as a related choice, most respondents ranked educating other (non-risk) employees on key risk management practices as the second performance gap. Taken together, filling these two gaps would go a long way toward integrating risk management into strategic planning – the top investment priority in 2020, as noted previously.

FIGURE 6

Lack of a formal ERM programme seen as biggest gap in many risk management functions.

Q: The biggest performance gaps in my organisation's risk management function involve...



Organisations seeking to strengthen or create an ERM programme should consider the following leadership traits and strategic approaches as they develop best practices:

- **Senior management support:** The enterprise risk manager – in some cases a chief risk officer (CRO) – has a seat at the table and a clear, direct line to both the C-suite and the decision-making authority.
- **Workflows:** Clear and articulated risk management workflows drive ERM best practices. All line-level staff support a culture of risk management and follow standard protocols.
- **Data:** Risk executives understand that knowledge comes from effectively managing data and are skilled in leveraging data models and trends.
- **Communication:** Enterprise risk leaders must be effective in communicating strategy in all forms, both internally and externally.
- **Process:** The ERM leader is process-driven and leads and collaborates, leveraging effective, proven management processes.
- **Reports:** There is effective reporting of complex information, throughout all levels of the organisation.
- **Technology:** ERM leaders can leverage technology and innovation and stay abreast of leading ways to incorporate technology into overall risk best practices.
- **Benchmark:** The ERM leader understands and balances the need and relevance of the benchmarking exercise and leverages benchmarking to advance strategic initiatives.

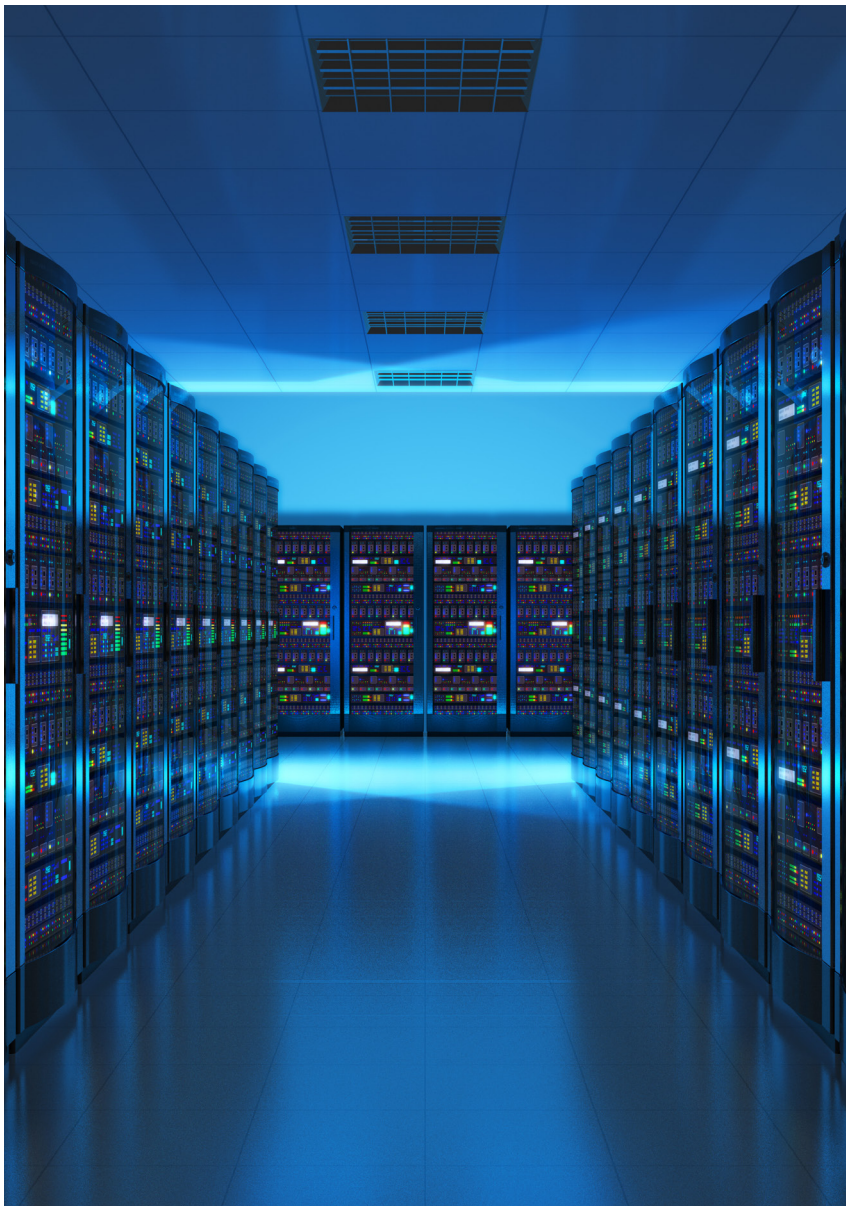
Adopting New and Innovative Solutions

The timely adoption of new/innovative solutions is another key challenge for the risk management function, with the performance gap in this area receiving the most overall votes among survey respondents. At a time when disruption is the norm, and in a technology-driven country such as India, this could prove a significant barrier at several levels, including around cyber risk.

According to the *2019 Global Cyber Risk Perception Survey*, many businesses are embracing technological innovation without adequately assessing the cyber risks of new technology. More than three-quarters of respondents cited at least one innovative operational technology – including cloud computing, proprietary digital products, and connected devices/IoT – that they have adopted or are actively considering.

And yet, while 74% of firms said they evaluate technology risks prior to adoption, just 5% said they evaluate risk throughout the technology lifecycle – and 11% do not perform any evaluation. An effective ERM programme can increase the likelihood that such evaluations will be ongoing.

Again, there is a clear disconnect between strategic decision-making relating to the risk management function at the C-suite level, and the realities of company-wide implementation felt by risk management departments. This is being felt across all levels of risk management development – organisations stand the risk of embedding this discrepancy into the foundations of their risk management practices and into their risk management culture.



Just 5% of firms said they evaluate risk throughout the technology lifecycle.

Insurance Solutions for Emerging Risks

Some of the most difficult events to prepare for fall under the banner of "emerging risks." Even defining the term can inspire differing opinions. Broadly speaking, emerging risks are viewed as having a high degree of uncertainty regarding their likelihood of occurrence, their interplay with other risks, and their consequences.

As with any risk, managing those considered "emerging" entails a risk finance component as part of overall preparedness and resilience. Given the nature of emerging risks, it's no surprise that just 28% of respondents said the insurance coverage available for emerging risks meets all of their organisation's needs, and 55% said it meets most, but not all (see Figure 7).

Looking back to the top risks identified by respondents, it's worth noting that either cyber-attacks or data fraud/theft were ranked as the number one priority by more than 70% of respondents, with extreme weather accounting for another 17%. These are high-profile emerging risks, with seemingly ever-increasing losses as technology opens up new cyber vulnerabilities and climate change heightens weather risks.

Only 7% of respondents believe that current insurance options do not meet any of their organisation's needs around emerging risks. And no chief executive officers or CROs held this view. At the same time, respondents who were treasurers or controllers said that available coverage meets some or all of their organisation's insurance needs for emerging risks. The survey shows that risk managers on the ground and those closest to their organisation's financial health were the only two groups to believe that the insurance coverage available in today's market does not meet their organisation's needs when it comes to key emerging perils like cyber and data-related risks.

In the same way that there is a divergence of views between the C-suite and risk managers with regard to performance gaps in risk management, these two groups are not aligned with regard to the effectiveness of current insurance coverage related to emerging risks.

When we asked specifically about business interruption coverage, 81% of respondents said they have fair or high confidence that their organisation's insurance programme will respond to claims. Of those with no confidence in the likely effectiveness of this coverage area, the respondents were either CROs, risk management executives, or chief financial officers.

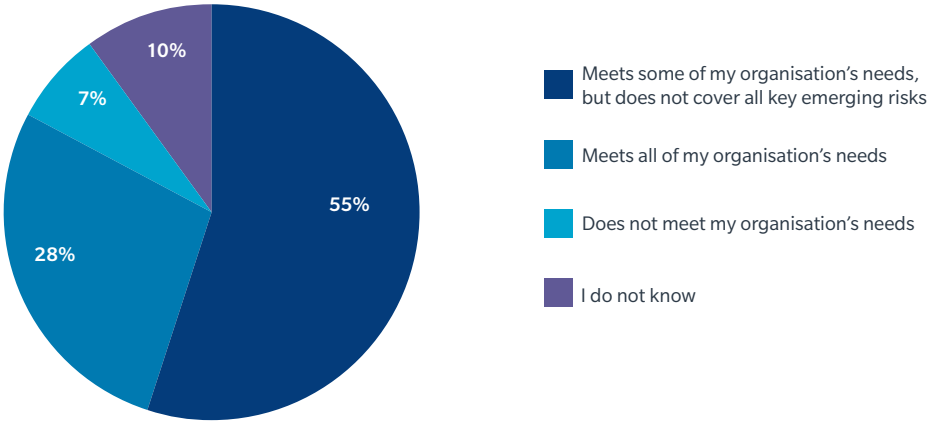
Business interruption is of heightened interest for some emerging and evolving areas, such as cyber risk. Cyber-attacks can seriously disrupt business operations, including at various points of the supply chain, both locally and internationally. Again, risk management executives and chief financial officers had no confidence in the available insurance provision; some CROs also had no confidence here.

Taking an enterprise-wide approach to risk management – with employees across the company playing an active role – will help prevent "blind spots" in an organisation's view of its risk management, including in its insurance coverage.

FIGURE 7

Less then one-third of Indian organisations say that insurance coverage for emerging risks fully meets their needs.

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



Recommendations

Foster collaboration around emerging risks

Understanding and managing emerging risks may require creative but pragmatic approaches that rely on cross-functional support across the organisation and senior-leader engagement.

Build an informed cybersecurity culture

Cybersecurity is likely at or near the top of your firm's risk agenda. From quantifying cyber risks to ensuring honest evaluations of cybersecurity posture, you can play an active part in developing and directing the strategy.

Seek a more strategic role for risk management

Improve the linkage between risk management and strategic planning with the use of data and analytics and assessment of risk management capabilities.

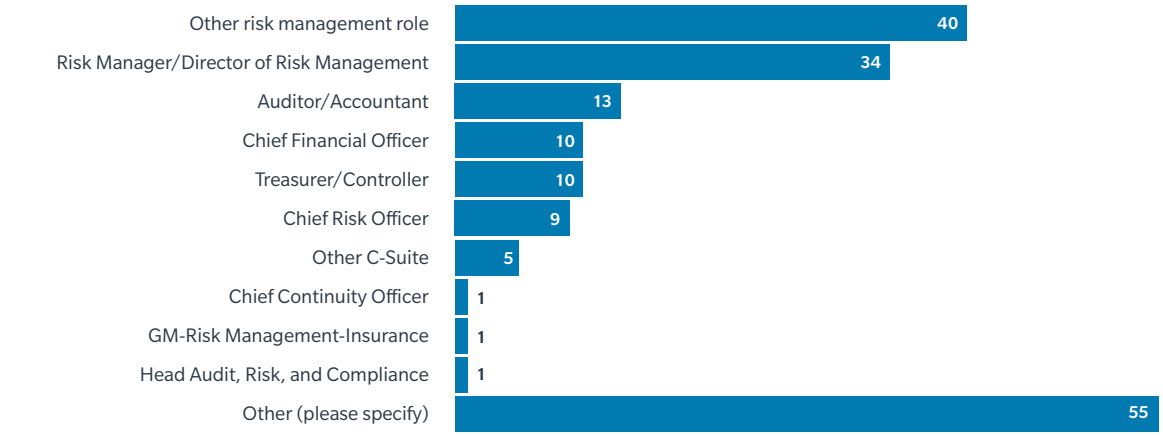
Focus your risk investment strategy

By maximising existing resources and advocating for effective new ones – including in risk transfer – you can strengthen your risk management department's role in the business.

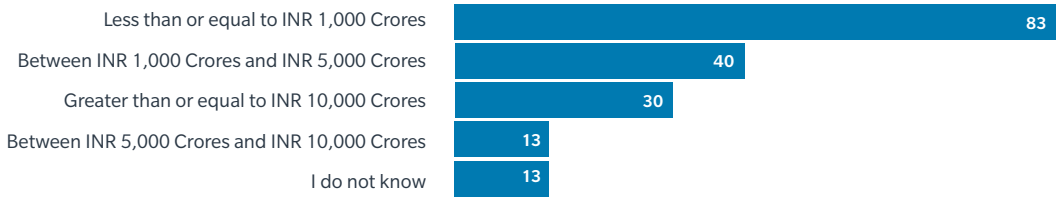
Survey Demographics

FIGURE 9 Profile of Respondents

Respondent roles



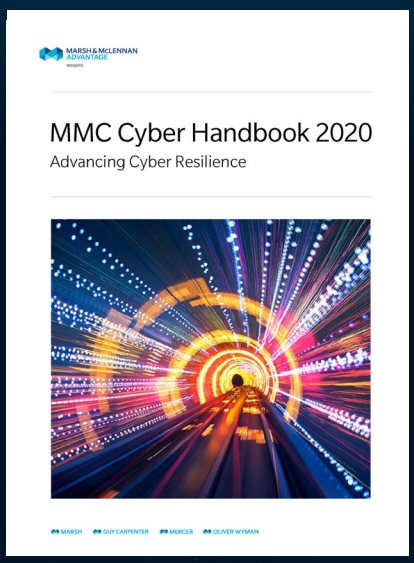
Organisation size, by revenue



Respondent industries (Top 10)

1	Financial Institutions/Services/Banking/Insurance
2	Communications, Media, and Technology
3	Manufacturing/Automotive
4	Power and Utilities/Energy
5	Construction/Engineering
6	Professional Services
7	Retail, Wholesale, Food, and Beverage
8	Pharmaceuticals
9	Health Care
10	Chemicals/Chemical Manufacturing

Recent Publications



Strategic Risk Finance in the Era of Big Data

The *2019 Excellence in Risk Management* report from Marsh and RIMS looks at how capital and data are changing the way risk managers understand and finance risk.

As the 16th annual *Excellence* report points out, there is a compelling relationship between understanding what alternative risk finance solutions can do and effective data and analytics. By leveraging data and grasping new risk finance opportunities, risk executives have an opening to become finance educators, adding value to the strategic decisions that affect their company's balance sheet.

2019 Global Cyber Risk Perception Survey

Cyber risk has moved beyond data breaches and privacy concerns to sophisticated schemes that can disrupt businesses, industries, supply chains, and nations, costing the economy billions of dollars and affecting companies in every sector.

The *2019 Global Cyber Risk Perception Survey* reveals many encouraging signs of improvement in the way that organisations view and manage cyber risk.

MMC Cyber Handbook 2020

Looking forward to 2020, we expect the cyber landscape to be more complex than ever before. The *MMC Cyber Handbook 2020* features perspectives from business leaders across Marsh & McLennan Companies, as well as strategic partners that represent some of the best thinking about the cyber economy.

This handbook brings together the latest perspectives on how to take action in the face of growing complexity and uncertainty, and dives into some of the most significant cyber trends, industry-specific implications, and emerging regulatory challenges.

“The survey found cyber-attacks emerging as a top risk concern for the second year in a row with awareness on the need to assess preparedness for digital threats.”

ABOUT MARSH

A global leader in insurance broking and innovative risk management solutions, Marsh's 35,000 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$15 billion and nearly 75,000 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.

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 be granted a composite broking license by the IRDAI. Currently, with presence in 17 branches across the country, with over 670 employees, and local market understanding backed by international expertise and global networks, it provides risk and insurance advisory to more than 4,900 clients in India. Follow Marsh India on LinkedIn.

ABOUT RIMS

RIMS, the risk management society®, is a global community of risk management professionals who are committed to advancing the profession through the exchange of ideas and best practices.

As the preeminent organisation dedicated to promoting the profession of risk management, RIMS, is a global not-for-profit organisation representing more than 3,500 industrial, service, nonprofit, charitable, and government entities throughout the world. Founded in 1950, RIMS is committed to advancing risk management capabilities for organisational success, bringing networking, professional development, and education opportunities to its membership of more than 10,000 risk management professionals who are located in more than 60 countries.

This report is a great example of the Society's thought-leading resources and content that empowers risk management professionals to become invaluable assets to their organisations.

ABOUT THIS REPORT

RIMS and Marsh have teamed up to help risk professionals understand the growing concerns of senior business leaders in India, to identify gaps in expectations and performance, and share opportunities to build stronger, more resilient risk management capabilities and organisations.

This report is based on 179 responses to an online survey with C-suite executives and risk professionals from leading firms across 23 industries conducted by Marsh and RIMS in August 2019, along with expert input from Marsh and RIMS.