INDIA

News&Views

CONTENT

Dear all,

As we continued to live through the pandemic, it was imperative to understand the new realities of doing business, accessing evolving risk and being resilient.

To ensure minimum disruption to client service, we at Marsh India made it a point to remain available to our clients through virtual communications platforms. Our colleagues are also helping them understand how insurance coverage may respond, manage claims processes and address effects on people and operations. Marsh is further focusing on its technology platforms to improve the delivery of our services and advisories to you. This will also allow seamless access to our global resources to your benefit.

I am pleased to share the current issue of our Newsletter – News & Views, which assesses the various aspects of cyber risks on the rise since the inception of the pandemic.

FEATURE: COVID-19: ASSESSING CYBER RISKS

Swift changes like the movement of a large portion of the workforce to remote working, telework and the expansion of e-commerce footprints had their inherent issues. These measures have caused many companies to implement new IT capabilities ad hoc. Some provisional solutions have bypassed normal development, approval and deployment processes, which have often stretched or violated existing cybersecurity policies while the activity of bad actors has increased globally. The article assesses how the incidence of cybercrime and cybersecurity issues have increased exponentially since the start of the pandemic and discusses the ways to be resilient.

FEATURE: PANDEMIC EMERGES AS THE TOP RISK CONCERNS FOR INDIAN COS: MARSH/RIMS STUDY

The continued effects of the COVID-19 pandemic, or a new public health crisis, emerged as the top risk concern for Indian companies according to a joint study conducted by Marsh, the world's leading insurance broker and risk adviser, and RIMS, the risk management society®. Results survey also show that large scale cyber-attacks and data frauds remain one of the top three risk concerns for the Indian corporate sector.

In the absence of physical events, Marsh India has initiated a Client Webinar Series to help clients with emerging risk solutions and policy implications post-COVID-19. This edition provides an update on our new Webinar Series: Excelling in Risk Management – The New Risk Order, conducted in October and November.

We welcome your feedback and encourage you to share it with us at contact.india@marsh.com

Warm regards,

Sanjay Kedia

SANJAY KEDIA
Country Head and CEO
Marsh India

COVID-19: ACCESSING CYBER RISKS

Pandemic-related restrictions have caused swift changes like the movement of a large portion of the workforce to remote working, telework and the expansion of e-commerce footprints. These measures have caused many companies to implement new IT capabilities ad hoc. Some provisional solutions have bypassed normal development, approval, and deployment processes, which have often stretched or violated existing cybersecurity policies at the same time that the activity of bad actors has increased globally.

These shifts have accentuated persistent and escalating cyber threats. Indian companies were forced to take quick steps to tackle the sharp escalation in cyber risk brought by the rapid and considerable shift to online business. According to various reports, as the pandemic unfolded from the beginning of the year, cyber crimes and ransom demands increased, with New Delhi among the top 101 most often attacked cities in 2020. Attackers used pandemic-related topics to launch phishing attacks, with more than a third of Indian respondents to a Microsoft survey2 saying they had fallen victim to such attacks.

Although, today's IT and network capabilities have enabled the strategies that have kept many companies afloat during the pandemic, the incidences of cybercrime and cybersecurity issues have increased exponentially.

This is because for hackers nothing changed: they always work from home. Working from home for them is a strength and for the normal employee, it is a new norm which can turn into a hacking opportunity.

HOW BIG IS THIS THREAT?

The current crisis has highlighted the need to prepare for serious business disruptions. A recent survey found that more than a fifth of organisations have shopped for new security solutions or services to respond to their new

reality. The global impact of the pandemic has prompted cybercriminals to modify their cybercrime campaigns to lure victims with pandemic themes and exploit the workforce mandated to work from home. This is across the segments, for instance:

- McAfee threat report 2020's detections of pandemic-related cyberattacks grew by an alarming 605% in the second quarter (April–June) alone.
- Science and technology sector accounted for a 91% rise in threat detections in the previous quarter.
- Incidents in manufacturing also increased by 10%.
- Attacks on cloud services users reached nearly 7.5 million in the second quarter.
- Malware-led attacks accounted for 35% of publicly reported incidents in the second quarter. Account Hijacking and Targeted Attacks accounted for 17% and 9% respectively.
- 419 new threats detected per minute on an average this quarter with new malware samples growing 11.5%.
- Ransomware attacks have **increased by 72%** during the pandemic.
- Ransom demands **rose 60%** to $178k from Q1 to Q2.
- Business downtime now averages **16 days:** 2+ weeks of operational disruption or impairment*.
- **Remediation and recovery costs** are growing with the use of new, more complex malware.
- Data exfiltration is increasingly used as a **coercion tactic** to encourage ransom payment.

Source: Coveware Q2 2020 Ransomware Marketplace report.

https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report

With employees, students, patients etc. asked to function remotely under stressful circumstances and infrastructure pushed to handle more activity, organisations must consider how their cyber risk profiles may be affected.

CHALLENGES AND SOLUTIONS

The biggest challenge is migrating from a physical presence to a virtual one. Once organisations acknowledge this

challenge, they must take appropriate action to mitigate potential risks. For example, by reinforcing employee and other users' awareness of cyber threats, boosting and supporting technology systems and reviewing insurance coverages with an eye toward potential losses under a cyber policy.

Awareness and Vigilance

Increased remote working is presenting more opportunities for cyber-attackers, and organisations just starting to use remote desktop protocols for work may be more susceptible to a cyber-attack. For instance, individuals may log in remotely from home networks that use less secure hardware.

Cyber actors have already taken advantage of people seeking information on the pandemic. COVID-19 is increasing the occurrence of phishing and "social engineering" events, with information about the virus used as the hook.

Remote working also increases the risk of relaxed privacy policies and procedures. To facilitate working from home, employees may remove printed files from the workplace or transfer personally identifiable information to unsecured or unencrypted storage or personal devices - potentially exposing the information to a breach by unauthorised users or improper use and disposal.

Organisations should proactively remind employees that good digital hygiene is even more critical when connecting to networks remotely. The burden may fall on employees at home to conduct activities such as patching

and updating systems, logging out when not working or using networks, physically securing computers, following proper procedures about handling private data and using robust passwords for devices and home wi-fi.

Demands on IT Resources

Organisations also need to maintain a heightened state of cybersecurity, including testing system preparedness for inevitable operational disruption. IT/InfoSec teams are being increasingly called upon to handle problems arising from a suddenly remote workforce.

The demand on web communication tools will increase, so system availability may be reduced. System outages or degradation will interrupt operations, causing loss of revenue and additional expense.

Insurance Considerations

Insurance coverage for privacy breaches, security incidents and technology outages is already available. A typical cyber policy provides various loss prevention and mitigation services that can be accessed both before and after an event. Several insurers are also proactively reaching out to policyholders when they become aware of potential threats or exploitable vulnerabilities.

However, with the unprecedented number of people "social distancing", the rapid rise of remote connectivity will likely create new vectors for cyber claims, particularly under three distinct coverages:

Most cyber insurance policies include a broad array of coverages that may be relevant given the current environment. These include:

- Network security liability,
- Privacy liability,
- Security response and forensic costs,
- Data recovery and restoration,
- Ransom event costs,
- Reputational harm,
- Network business interruption and associated expense,
- System failure,
- Contingent business interruption,
- Privacy regulatory defence.

POLICY LIMITATIONS

Cyber policies: May contain infrastructure exclusions, voluntary shutdown coverage limitations, and limitations in a computer system, network, and system failure definitions that could affect how coverage applies.

Infrastructure exclusions. Policies typically exclude coverage for failure of power, utility, mechanical or telecommunications (including internet) infrastructure or services not under the insured's direct operational control.

Voluntary shutdown coverage limitations. Coverage may only apply to voluntary shutdowns to prevent the spread of malware or limit damage—and not to shutdowns intended to improve network access or functionality.

Limitations in a computer system or network definitions. Policyholders should review key definitions and whether they affect coverage for owned, operated, or leased systems and those operated by third parties.

Limitations in system failure definitions. Some policies may require a human or programming "error", proof of testing or patches or proof of system used before failure to trigger coverage.

CONCLUSION

Cybercrime is becoming a greater risk when doing businesses for all industries in the Asia Pacific (APAC) as compared to North America and Europe. Rapidly growing connectivity and the accelerating pace of digital transformation expose the region and make it particularly vulnerable to cyber exploitation.

Cyber insurance not only provides a comprehensive cover for the financial losses but also pays for service providers, which include a team of lawyers and public relations experts to help you manage a cyber-attack event effectively.

Reference:

1. Subex Releases Q2FY21 Threat Landscape Report - Subex Limited

2. Exploiting a crisis: How cybercriminals behaved during the outbreak - Microsoft Security.

BY **RITESH THOSANI**
Vice President, Cyber Specialist
Marsh India

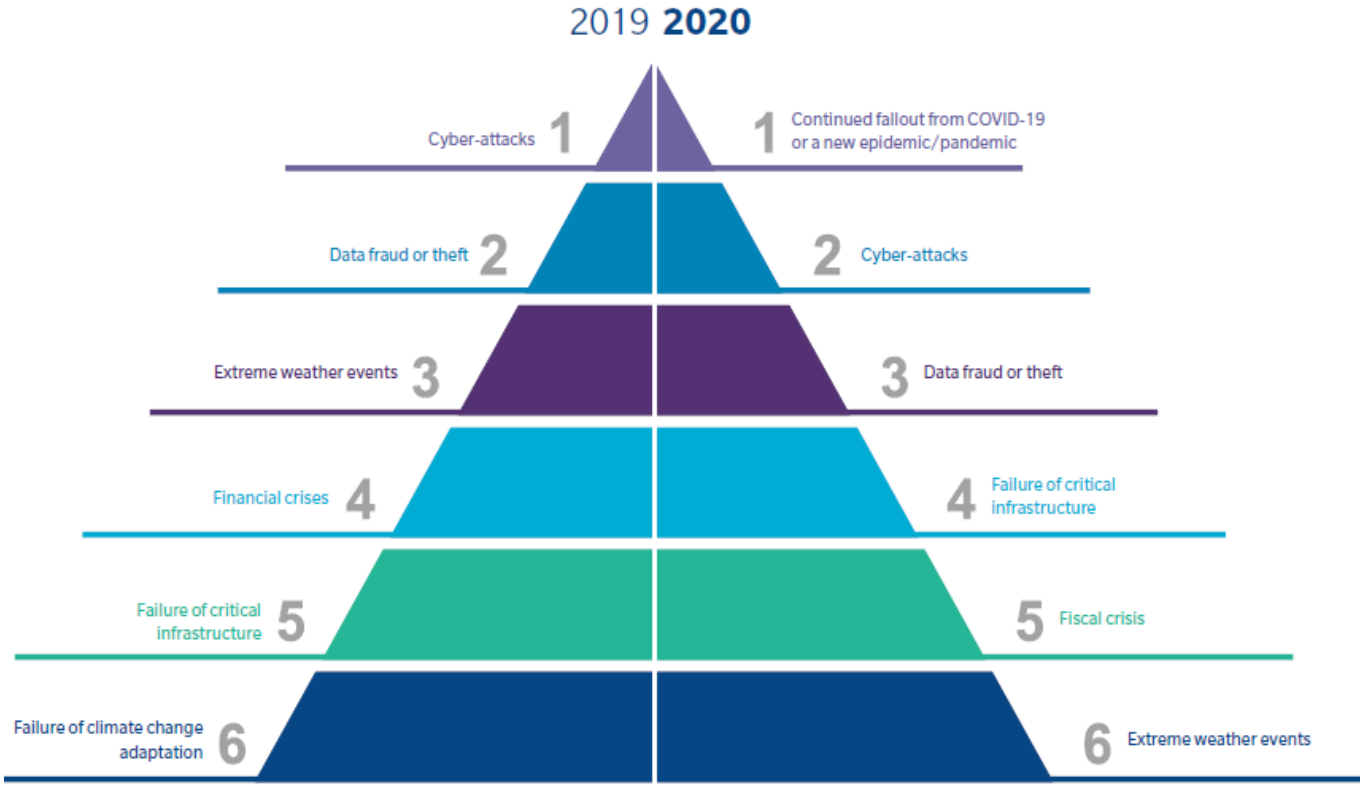
PANDEMIC EMERGES AS THE TOP RISK CONCERNS FOR INDIAN COMPANIES:MARSH/RIMS STUDY

The continued effects of the COVID-19 pandemic, or a new public health crisis, emerged as the top risk concerns for Indian companies, according to a joint study conducted by Marsh, the world's leading insurance broker and risk adviser, and RIMS, the risk management society®.

Results from the *Excellence in Risk Management India 2020, Spotlight on Resilience: Risk Management During COVID-19* survey also show that large-scale cyber-attacks and data frauds remain one of the top-three risk concerns for the Indian corporate sector. While there is great optimism about the ability of organisations to rebound and address future pandemic-related challenges, cyber-attacks and data fraud continue to be paramount concerns for risk professionals in India.

According to the report, around 63% of the 231 survey respondents, which included C-suite executives and senior risk professionals, identified a new pandemic or continued fallout of COVID-19 among the top three risks facing their organisation. Cyber attacks (56%), data fraud or theft (36%), failure of critical infrastructure (33%), fiscal crises (31%), and extreme weather events (25%), were highlighted among the other top risks for Indian businesses. The majority of survey respondents (85%) said the pandemic necessitated a shift to remote work, a move that has increased their organisations' exposure to a potential cyber-attack.

Extreme weather events drop in priority.



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

In the light of the ongoing pandemic and shutdowns imposed by national and local governments, a failure of critical infrastructure climbed the ranks in the 2020 survey, as many organisations re-evaluated their risk management priorities. Despite various extreme weather events, such as cyclones and forest fires, extreme weather dropped from third in 2019 to sixth in 2020.

This year's events emphasised the need to be proactive. The importance of risk management has come to the fore, with an emphasis on the value of robust business continuity plans that quickly and effectively respond to challenges. As the risk management community becomes more informed, it should become better prepared to support strategic decision-making.

However, to be proactive, organisations need to develop processes and channels to collect and review critical information. Building risk-aware, collaborative organisational cultures will allow organisations to plan for interconnected risks and to leverage previously unrealised opportunities.

"Organisations need to balance their focus between longstanding and emerging risks. While there has long been an awareness of weather-related risks, low-frequency risks generally receive less attention. The pandemic has underlined the need for risk managers to keep all perils on their radar," said Sanjay Kedia, Country Head and CEO, Marsh India.

This year's report examined the need for building organisational resiliency to a variety of low-frequency but high-severity risks. However, while many senior business leaders are shifting attention to questions of resilience, more than one-fifth of respondents said that they do not assess or model emerging risks.

"Organisations need to focus on building resiliency to future black swan events. The lessons learned in 2020 should be leveraged to revise business continuity plans so that companies can withstand the impact of the next big challenge," Mr Kedia added.

ABOUT THIS REPORT

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

This report is based on 231 responses to an online survey with C-suite executives and risk professionals from leading firms across 26 industries conducted by Marsh and RIMS in August 2020, along with expert inputs from Marsh and RIMS specialists. We hope that in the coming years, we can further expand and deepen the findings of this survey.

MARSH IN THE MEDIA

AUGUST

AUG 3

Sanjay Kedia, Country Head and CEO, Marsh India shared his views with Asia Insurance Review in a recent article titled, "**Prepare for post pandemic or perish**". The featured article talks about how the COVID-19 pandemic has fast-tracked the process of digitisation in the insurance industry and the Indian insurance broking industry is adapting to meet those emerging needs of policyholders post-pandemic.

"Many perceive digital/online to be a threat for the intermediaries, however, it provides a massive opportunity for us," Sanjay said.

Link: https://www.linkedin.com/feed/update/urn:li:activity:6696274895094980608

AUG 6

Bhishma Maheshwari, Executive Vice President, FINPRO, Marsh India co-authored an article on cyber risks in India for Norton Rose Fulbright. The article, titled, ***An analysis of international cyber risks faced by Indian businesses and risk management strategies***, discusses various legal, underwriting and insurance broking perspective while dealing with international cyber risks faced by Indian businesses.

Link: https://www.linkedin.com/feed/update/urn:li:activity:6697157377189269504

OCTOBER

OCT 1

Marsh India issued a press release announcing the completion of JLT Independent buy. The release titled, "**Marsh India completes acquisition of JLT Independent**", was carried by 1 Wire and 6 online publications.

Link: https://www.outlookindia.com/newsscroll/marsh-india-completes-acquisition-of-jlt-independent/1946741

OCT 8

Marsh issued a press note titled, **"Unemployment, infectious diseases emerge as top challenges for business leaders: WEF survey"**, based on the findings of the new WEF report. The news was covered by more than 120 publications including, **3 Wires and 25 International and 95 National coverage online coverage.**

Link: Unemployment is world's biggest risk, business leaders say

https://timesofindia.indiatimes.com/business/international-business/unemployment-is-worlds-biggest-risk-business-leaders-say/articleshow/78551500.cms

DECEMBER

DEC 1

Sanjay Kedia, Country Head and CEO, Marsh India shared his views with Asia Insurance Review in a recent article titled, "**COVID-19: A pre-existing disease**". The featured article talks about how would insurers classify COVID as a pre-existing condition and strike a balance between onboarding those infected by COVID-19 and their own sustainability without bringing COVID-19 into the category of pre-existing disease.

Link: https://www.linkedin.com/feed/update/urn:li:activity:6739464878882349056

NEWS AND INSIGHTS

1. MARSH INDIA COMPLETES ACQUISITION OF JLT INDEPENDENT

Marsh India announced that it has completed the acquisition of the insurance broking operations of JLT Independent Insurance Broking. Earlier, the two companies received approval for the transaction from the Insurance Regulatory and Development Authority of India.

"The transaction follows the acquisition of JLT Group by Marsh & McLennan Companies on April 1, 2019," Marsh India said in a statement, adding that it will also help strengthen its position in the country. *READ MORE*

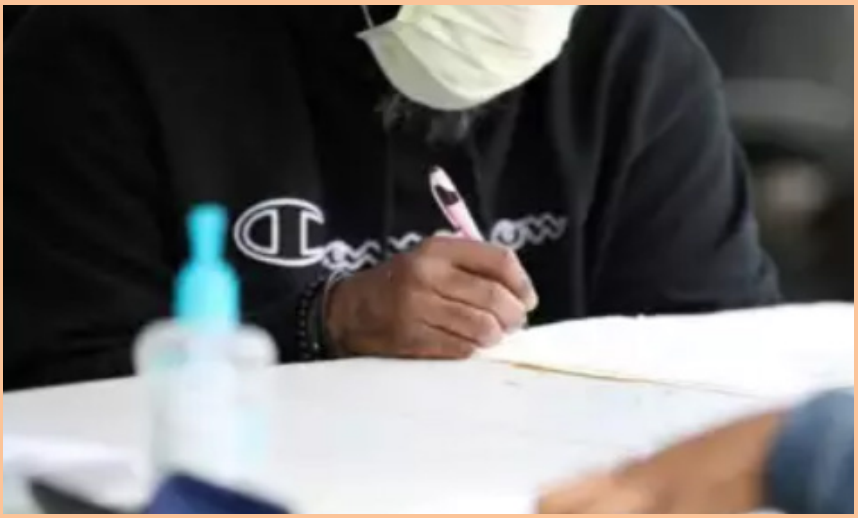
2. UNEMPLOYMENT IS WORLD'S BIGGEST RISK, BUSINESS LEADERS SAY

Unemployment is seen as the biggest worry over the next 10 years for business executives around the world, closely followed by concern about the spread of infectious diseases, according to a survey by the World Economic Forum. Unemployment rates have rocketed due to lockdowns and other restrictions to combat the coronavirus pandemic, with fears of worse to come in countries which have furloughed workers.

"The employment disruptions caused by the pandemic, rising automation and the transition to greener economies are fundamentally changing labour markets," said Saadia Zahidi, Managing Director at the World Economic Forum (WEF). *READ MORE*

3. FINMIN INVITES BIDS FROM ACTUARIAL FIRMS FOR VALUING LIC AHEAD OF IPO

The government has invited bids from eligible companies for the appointment of an actuarial firm to determine the embedded value of Life Insurance Corporation of India, taking the next step towards the public listing of the country's largest public insurer. LIC needs to develop an Indian Embedded Value (IEV) reporting framework for the necessary disclosures in the proposed initial public offer, the Department of Investment and Public Asset Management said in its request for proposals recently. *READ MORE*



4. CYBERSECURITY, DATA PROTECTION MUST PROMOTE FINANCIAL INCLUSION: RBI GUV

Issues concerning cybersecurity and data protection must be addressed to gain the confidence of the excluded section in the use of technology, which is necessary for promoting financial inclusion, Reserve Bank Governor Shaktikanta Das said recently. "Technology, though being a great enabler, can also lead to exclusion of certain segments of society," Das said in his keynote address at a webinar on "Investing in Investor Education in India: Priorities for Action", organised by the NCAER. The RBI Governor added that it was imperative to build trust in formal financial services among the hitherto excluded population. *READ MORE*

5. US OFFICIALS SUSPECT RUSSIAN HACKERS BROKE INTO FEDERAL AGENCIES, KREMLIN DENIES ACCUSATIONS

Hackers believed to be working for Russia have been monitoring internal email traffic at the U.S. Treasury Department and an agency that decides internet and telecommunications policy, according to people familiar with the matter.

There is concern within the U.S. intelligence community that the hackers who targeted the Treasury and the Commerce Department's National Telecommunications and Information Administration used

a similar tool to break into other government agencies, according to four people briefed on the matter. The people did not say which other agencies. Three of the people familiar with the investigation said Russia is currently believed to be behind the attack. *READ MORE*

6. TATAS, INTERUPS AMONG 'MULTIPLE' BIDDERS FOR AIR INDIA

Salt-to-software conglomerate Tata Group and US-based fund Interups Inc were among "multiple" entities that on Monday put in preliminary bids for buying loss-making carrier Air India. A group of 219 Air India employees submitted an expression of interest (EoI) for the carrier in partnership with Interups at the close of the deadline on Oct 14, news agency PTI reported: "Multiple expressions of interest have been received for strategic disinvestment of Air India. The Transaction will now move to the second stage," Department of Investment and Public Asset Management (DIPAM) Secretary Tuhin Kanta Pandey tweeted.

He, however, did not reveal either the identity of the bidders or the number of bids received for buying the national carrier. *READ MORE*

7. OAKTREE CAP EMERGES AS THE HIGHEST BIDDER FOR DHFL

Global alternative asset investor Oaktree Capital Management has emerged as the highest bidder for bankrupt Dewan Housing Finance Corp. Ltd (DHFL), beating Adani Enterprises Ltd and Piramal Group, newspaper Hindustan Times reported citing unnamed sources.

Oaktree Capital offered to pay Rs32,700 crore in the fourth round of bidding for mortgage lender DHFL's entire portfolio, followed by Piramal with Rs32,350 crore and Adani Enterprises with Rs29,860 crore, the people cited above said on condition of anonymity, the report added. *READ MORE*

8. IRDAI TO BAN CREDIT-LINKED GROUP HEALTH INSURANCE

Insurance regulator Irdai has proposed a ban on credit-linked group health policies such as critical illness covers that are bundled with home loans. According to industry sources, the products that are pushed to homebuyers are mis-sold as health covers. Irdai has proposed that all existing credit-linked group health policies be withdrawn by December 31, 2020.

"As the primary purpose of any health cover is to meet the treatment costs or to manage the lifestyle on the diagnosis of critical illness, no insurer is permitted to offer any indemnity or benefit-based credit-linked group health products," Irdai said in a draft circular. The regulator has, however, made an exception for the sale of personal accident policy. *READ MORE*

9. INDIAN COMPANIES PAID UPTO $2.5 MN TO GET BACK DATA FROM HACKERS: REPORT

Indian organisations were hit hard by ransomware attacks in 2020. Globally, India Inc stood second when it came to ransom pay-outs and more than a third paid between $1 Mn - $2.5 Mn to hackers for such cyberattacks. These numbers were

revealed by the US cyber tech firm CrowdStrike after a global survey. The 2020 Global Cyber Security Attitude Survey also found that India Inc is particularly threatened by cyber attacks originating from China and Pakistan due to rising geopolitical tensions.

While 74% organisations in India suffered a ransomware attack, the numbers were 67% in Australia, 52% in Japan and 46% in Singapore in the APCA region. *READ MORE*

COMPILED BY MARSH INDIA COMMUNICATIONS TEAM

EVENTS AND WEBINARS

As the COVID-19 situations intensified across India and the measures, such as lockdown disrupted businesses and economy, Marsh India initiated client Webinars as one of the ways to improve client engagement during this period.

Accordingly, with the physical events not possible, Marsh India initiated Client Webinar Series to help clients with emerging risk solutions and policy implications post COVID-19 Pandemic.

WEBINAR UPDATE: **APRIL - DECEMBER**	
Number of Client Webinars	49
Questions Answered	1000
Number of Atendees	10500

Marsh has created a coronavirus microsite, which has country-specific pages. All the Marsh India advisories and webcasts are now uploaded on this website.

MARSH INDIA COVID-19 ADVISORIES

All the Marsh India client advisories related to COVID-19 are now hosted on the India page under Research & Briefing section.

To know more please visit:

https://coronavirus.marsh.com/sg/en/india.html

WEBCAST LINKS

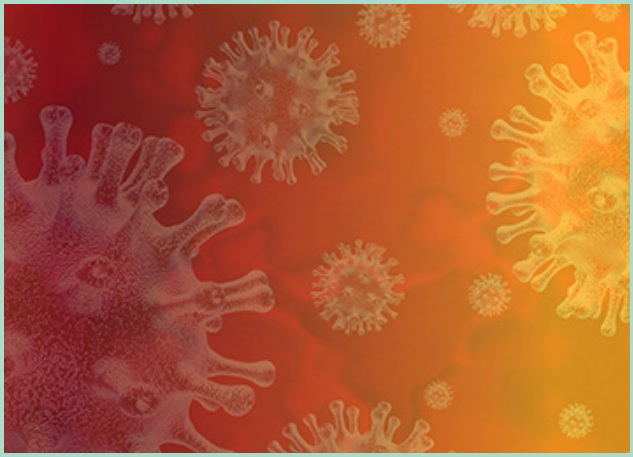
On the same page, we have a created a separate drop-down tab Webcasts under the Insights tab.

All the webinars links are uploaded here:

https://coronavirus.marsh.com/sg/en/insights/webcast.html

MARSH INDIA #WEBINAR SERIES EXCELLING IN INSURANCE AND RISK MANAGEMENT

Marsh India recently organized a Webinar Series – ***Excelling in Insurance and Risk Management***, which showcased the best of MARSH Global capabilities to our clients. The idea was to arrange a Masterclass on key risk issues important to clients and colleagues by Marsh global leaders/experts.



Webinars Conducted:

Webinar #1: The New Risk Order: Mental Health & Wellbeing – Oct 9, 2020

GLOBAL EXPERT: **Dr. Wolfgang Seidl**; Partner, Workplace Health Consulting Leader UK and Europe, MMB

Webinar #2: The New Risk Order: Trade Credit Risks, on Oct 13, 2020

GLOBAL EXPERT: **Tim Smith**, Global Trade Credit Leader UK, **Tyler Wendleken**, Trade Credit Leader Asia

Webinar #3: The New Risk Order: Resilience and Emerging Risks, Oct 14, 2020

GLOBAL EXPERT: **Michael Poulos** - Global Head, CAS Marsh, **Paul Wilkins** - RMP Leader Asia, Marsh

Webinar #4: The New Risk Order: BI Risks & Insurance Claims, Oct 20, 2020

GLOBAL EXPERT: **Seth Peller**, North Asia CCO, **Dennis Dalati**, Head – Asia Claims. Global Claims Practice

Webinar #5: The New Risk Order: Evolving D&O Risks and Insurance Solutions, Oct 22, 2020

GLOBAL EXPERT: **Shaunna Batabyal**, Vice President, Head of International Management Liability, Marsh UK, **Sharon Kerr**, Managing Director, Deputy FINPRO Leader Asia

Webinar #6: The New Risk Order: Cyber Resilience Nov 2, 2020

GLOBAL EXPERT: **Thomas Reagan**, Cyber Practice Leader, US, **Magda Chelly**, Head - Cyber Risk Consulting, Asia

Webinar #7: The New Risk Order: Parametric Solutions, Nov 3, 2020

GLOBAL EXPERT: **Ben Qin**, Asia Pac Leader, **Paul Wilkins**, RMP Leader Asia

Webinar #8: The New Risk Order: Risk Finance Optimisation, Nov 6, 2020

GLOBAL EXPERT: **John Davies**, Global Head of Analytics

To listen to all our webinars, please visit: https://coronavirus.marsh.com/sg/en/insights/webcast.html

We hope through such webinar sessions would help our clients to be more resilient in the face of the emerging and increasingly interconnected risks landscape.

COMPILED BY MARSH INDIA COMMUNICATIONS TEAM

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 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 BRINK.

Marsh India Communications Team.

For any information, please contact:
NILADRI BHATTACHARYA
niladri.bhattacharya@marsh.com

MARSH

MUMBAI (HEAD OFFICE)

1201-02, Tower 2, One World Center, Jupiter Mills Compound, Senapati Bapat Marg, Elphinstone Road (W), Mumbai 400 013, India.
T: +91 22 6651 2900
T: +91 22 6651 2901

BENGALURU

Alamelu Terrace, 3rd Floor
163, Annasalai Opp.
Spencer plaza
Chennai - 600 002
T: +91 44 4348 6969
F: +91 44 4348 6965

GIFT CITY OFFICE (GANDHINAGAR)

4th Floor, Signature Building
Premise No 409, Block
13-B Zone 1, Gift City, SEZ,
Gandhinagar,
Gujarat 382 355, India.
T: +91 79 6180 0205

HYDERABAD

203, 2nd Floor, Ashoka Vishnu Capital, Plot No: 90,
Road No: 2, Banjara Hills,
Hyderabad 500 034, India.
T: +91 40 4664 8800
T: +91 40 4664 8888

NOIDA

2nd Floor, 91 Springboard,
Sector C-2, Noida 201 301,
India.
T: +91 88 6066 1763

ANDHERI

3rd Floor, Fleet House (Next to Marol Metro Station), Opposite Marol Fire Station, Andheri Kurla Road, Andheri East,
Mumbai 400059, India.
T: +91 22 6835 2500

CHENNAI

Alamelu Terrace, 3rd Floor,
#163, Annasalai Opposite
Spencer Plaza,
Chennai 600 002, India
T: +91 44 4348 6969
T: +91 44 4348 6965

GURUGRAM

Unit-I, 7th Floor, Tower-A
DLF Infinity Towers, DLF Cyber City, Gurugram 122 002, India.
T: +91 124 4049 200
T: +91 124 4049 201

INDORE

Regus, DNR90, Unit Nos. 301,
3rd Floor, 569/3, MG Road,
Indore, India.
T: +91 731 478500
T: +91 91 6798 0179

PUNE

91 Springboard, 3rd Floor,
Clockhouse, Creativity Mall,
Shastrinagar, Off. Airport Road
Yerawada, Pune 411 006, India.
T: +91 77 3850 0678

AHMEDABAD

1001, 10th Floor, Sun Avenue One, Opp. Shreyas Foundation Back Gate, Manekbaug to Shyamal Road, Satellite, Ahmedabad 380 015, India.
T: +91 89 8003 3279

DIBRUGARH

H/No: 12, Dharmapara
Graham Bazar Tinali,
Dibrugarh 786 001, India.
T: +91 83 3607 6009

GURUGRAM 2

91 Springboard Business Hub Private Limited 145,
Sector 44 Rd, Sector 44,
Gurugram 122 003, India.
T: +9 1 88 6066 1763

KOLKATA

PS Arcadia Central Unit # 2C,
2nd Floor, 4A, Abanindranath Thakur Sarani (Camac Street),
Kolkata 700 017, India.
T: +91 33 3984 5212
T: +91 33 3984 5248

VADODARA

Office No. 203, Hari Bhakti Extension Colony, Near Malhar Point Old Padra Road,
Vadodara 390 007, India.
T: +91 0265 302 3898
T: +91 0265 302 3898