

CYBERSECURITY PRIORITIES AND BUSINESS IMPLICATIONS IN A POST COVID WORLD

An exclusive survey report by BDO in India
in association with CII



April 2021



FOREWORD

The COVID-19 pandemic brought significant changes in everyone's personal and professional life. It also uplifted online education, hygiene habits and brought us closer to our families. The restrictions imposed by the various governments in response to the pandemic has forced us to segregate the physical perimeters of working from an office- and transitioned us to work from home environment. Eventually, work from home has become more prevalent and efficient than ever before. In adherence to the regulatory and compliance requirements, security came at the forefront, thereby increasing the challenges faced by CxO and the board of directors.

Due to office space transition, there has been a surge in cyber-attacks during the COVID-19 pandemic. Companies are fast-tracking their digital transformation, and cybersecurity is now a significant concern. Ransomware and Social Engineering attacks have increased exponentially over these times, impacting businesses of all sizes and sectors. Cyber-attacks have resulted in considerable damage from financial losses, operational service disruption, and the erosion of shareholders' trust. Governments worldwide are re-evaluating ways to ensure stability and upward graph for the economy and smooth operation of businesses in a cyber-safe environment, especially in the healthcare sector.

Regardless of global events, security threats continue to exist and grow in IT systems, and ongoing efforts are needed to ensure these are addressed before attackers exploit them. Organizations may not effectively detect cyber-attacks as security teams are short-staffed or repurposed to support other activities, leaving security alerts uninvestigated.

As organizations move away from their secured physical office space and become increasingly reliant on remote access technology, any disruption caused by cybersecurity attacks or IT outbreaks will significantly impact operations, delivery, and performance.

Due to these large-scale attacks, organizations have realized the importance of Cyber Insurance to protect them from future cyber threats and limit their liability. This report aims at unveiling the impact of COVID-19 on cybersecurity and its business implications. It also emphasizes the importance of enterprise risk management and cybersecurity strategies for the future. We trust this publication will provide an insight into the future of cybersecurity.



MUBIN SHAIKH

Partner & Leader/ Cyber Security
Business Advisory Services
BDO in India

**RAJAN NAVANI**

Chairman- CII WR Sub-committee on Innovation,
Technology & Digitization
Chair, CII Council on India@75
Vice Chairman & Managing Director- JetSynthesys

FOREWORD

The Confederation of India Industry (CII) is an organization that works to create and sustain an environment conducive to India's development, partnering industry, government, and civil society, through advisory and consultative processes. It has contributed towards conducting several cybersecurity events and conferences remotely throughout 2020 amid the COVID-19 lockdown. On numerous occasions, it collaborated with BDO India LLP in conducting a survey based on the impact of COVID-19. Basis the survey results showed that high profile businesses and government organizations were increasingly targeted by cybercriminals, causing a substantial financial and reputational loss. While we continue strengthening our cyber defenses, attackers continually develop new and more sophisticated methods to breach the enterprise network in a bid to control technology assets and compromise critical data.

The Indian government is currently pushing towards a massive digital revolution with the Digital India initiative by introducing smart cities and e-governance. With increasing digital platforms, there is an increase in attack surfaces for the attackers, thereby leading to a significantly higher number of threats and vulnerabilities in an organization's current IT infrastructure. People who are unaware of such an attack's risk and possible impacts are the most vulnerable and weakest link in any organization. The attackers take undue advantage of this through social engineering-based attacks.

With the rise in adversaries and an amalgamation of sophisticated attack vectors, access to encrypted data has become easy, so has the sale of sensitive data on the dark web. This gives rise to a massively increasing number of cybercrimes, hampering organizations' ability to effectively engage in risk management activities and implement necessary security measures to safeguard their data.

The COVID-19 pandemic forced everyone around the world to work from home instead of an office-based setup, thereby shifting from a LAN based network to a VPN based network. Due to such a transition, there may be security patches that were not updated—leaving a loophole for the adversary to take advantage and exploit the network. All arrangements made for remote working has brought security to the forefront. These concerns can be addressed by implementing and maintaining a robust Risk Management strategy.

EXECUTIVE SUMMARY

In the era of digital transformation, the global pandemic acted as a catalyst in shifting the work from office culture to a work from anywhere set up. During pre-COVID-19 times, security was assured due to proper office-based equipment from a designated office premise. However, now, enterprise protection mechanisms and controls are deployed to ensure employee systems are secured from targeted phishing campaigns that could lure them into clicking on unknown links and attachments.

It is evident from the survey that maintaining these controls during the pandemic has become a challenge. In a nutshell, the report provides a holistic view of an organisation's challenges and the efforts undertaken to reduce these challenges and the accompanying risks.

The remote working norm has increased the number of cyber threats and the possible attack surface for attackers. Social engineering attacks such as Phishing attacks can reveal username, password, bank account details, etc., to the attacker by clicking on a malicious email attachment, link, or responding to fraudulent emails.

While organizations offer Virtual Private Network (VPN) access to their employees, the first point of interface for laptop or desktop is typically a broadband network, mobile hotspot, or shared wireless network. Employees connect to these devices via home wireless routers, which have rudimentary security for encryption of traffic. Some of the devices also have default passwords for an administration, that are left unchanged. When a remote user clicks on a suspicious link, they are redirected to a malicious website, leading to loading malicious executable codes on a corporate laptop's browser, leading to a compromised enterprise network. This malicious code could also extract valid corporate credentials when a user logs into the enterprise portal or application.




**CYBERCRIME IS A
CONSTANTLY
EVOLVING AND
EVER-INCREASING
CHALLENGE FOR
BUSINESSES
TODAY**

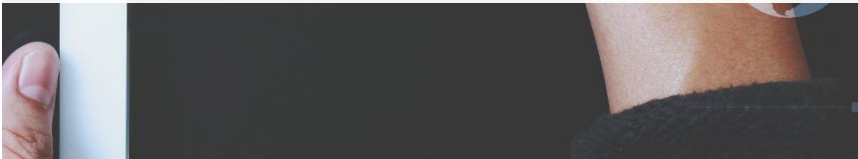
To stop or control these crimes, each organisation should have an enterprise risk management strategy. All organisations should prepare a risk management plan to protect their critical information from getting exposed to unauthorised users/intruders/attackers. A very well thought, organised, and executed plan will avoid data breaches. A plan-based business strategy aims to identify, assess, and prepare for any danger and other potential threats.

The need for a risk management strategy has never been so critical. A firm cannot define its goals and objective unless the risk management plan is adopted. The organisation should detect, analyse, and mitigate the risk to achieve the desired goals efficiently. Risk avoidance, acceptance, transfer, and monitoring are risk mitigation steps. The potential risk could affect any combination of performance, cost, and scheduling, thereby emphasising the use of different strategies to address threats based on impact. It is the responsibility of all organisations to plan their future strategies to execute their business operations smoothly. Suggestions are being made to organisations for mandatory 'cyber insurance' which shall cover malicious activities performed by hackers and cybercriminals. It is a risk management technique where cyber risk is transferred to an insurance company, further returning the lost revenue. Advanced technologies such as Cloud Computing, Machine Learning, and Artificial intelligence should be used for data storage as there are very few data loss chances or data breaches.

COVID-19 continues to cause unprecedented disruption to organisations. These issues are unlikely to subside in the near term. Therefore, organisations need to prioritise the continuity of their critical functions and remain flexible in how they operate. Consequently, many organisations will require employees to Work from Home (WFH).



Highlighted here are important questions that management should relay at board meetings to establish a secure way forward in the new normal:

- ◆ Do employees who are performing a critical function have an alternate means of connecting to the internet?
 - ◆ Have you reminded employees to backup and save their work if a connection is lost, interrupted, and/or not responding?
 - ◆ Have you provided your employees with a secure way of connecting into your business environment, such as a VPN?
 - ◆ Have you reminded staff of the acceptable user policy for work-issued devices?
 - ◆ Have you validated that user accounts are separated from admin accounts?
 - ◆ If during WFH arrangements, employees are required to use their personal mobile phones, have you considered mobile device management?
 - ◆ Is there a specific process or procedure for running backups?
 - ◆ Have you reminded employees about the importance of remaining vigilant to suspicious emails, especially COVID-19 emails/SMS?
 - ◆ Has your organisation implemented phishing awareness programs?
- 

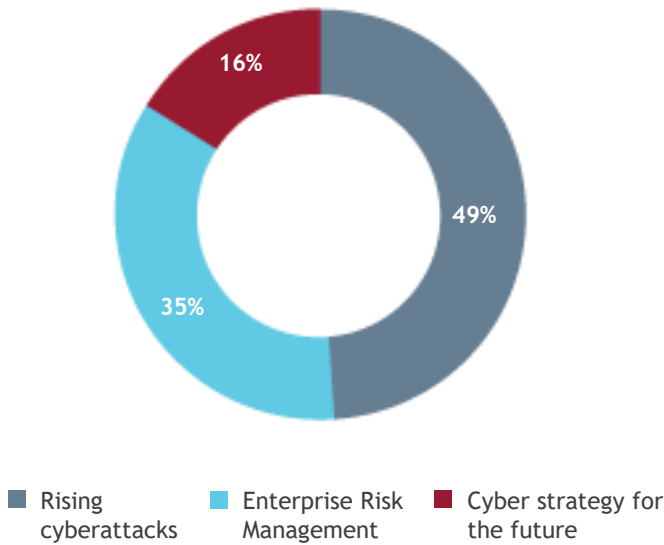
ABOUT THE SURVEY

BDO in India in partnership with CII conducted a survey on the impact of COVID-19 on cybersecurity priorities and the business implication. The survey aimed at understanding the rising cyberattacks globally, the perception of Enterprise Risk Management (ERM) in securing data, and the future cyber strategies to control the risks.

TARGET AUDIENCE

Employees
Managers
Board of directors

THE SURVEY FOCUSED ON THREE IMPORTANT THEMES



The COVID-19 pandemic has given rise to many cyberattacks. It was observed that around 49% of the firms surveyed were affected and suffered from risks and damages such as sensitive data loss, disruption of business/service, financial impact etc. Due to the pandemic and the uncertainty that followed, organisations cutdown on spends including cybersecurity budgets. Many respondents believe that the remote working arrangement has further increased the chances of cyberattacks.

ERM is a mandatory process for all firms. About 35% of the respondents have effective risk management strategies at their organisations. Given the current situation some firms have opted for a cyber review, while others have not considered that option yet. Out of the total responses, only 46 respondents have an ERM framework that covers risks like the current COVID-19 pandemic. Many firms have also updated their ERM framework.

According to the survey, only 29 respondents out of the total respondents suggested that their firms have cyber insurance while 54 respondents are still unsure about the same. There are 32 firms where cyber insurance is not a part of their strategy and 31 others who are planning to buy a cyber insurance soon. The other respondents are looking at revamping the existing business continuity plan or use Robotics Process Automation (RPA). Use of cloud software as a service (SaaS) is the future strategy for majority of the firms, as it can store a large amount of data with high amount of security measures.

**RISING
CYBERATTACKS**

**ENTERPRISE RISK
MANAGEMENT**

**CYBER STRATEGY
FOR THE FUTURE**



RISING CYBERATTACKS



NIPUN JASWAL
Director / Cyber Security
Business Advisory Services
BDO in India

For most of 2020, the COVID-19 pandemic disrupted normal life and compelled people across the globe to stay home and transition to a Work from Home (WFH) environment. Throughout the year, most organisations' IT teams faced the pressure of enabling this sudden transition from a secure work culture from a typical office setting to work from anywhere. While few organisations enabled VPN for their employees in a secure manner, most businesses were compelled to take the digital plunge without much preparation, thus neglecting security concerns and resulting in a massive rise in cybercrimes. As per our survey results, 72% of the respondents confirmed that their organisations faced a cyberattack during the COVID-19 phase, while 8% of the respondents weren't aware of such attacks in their organisations.

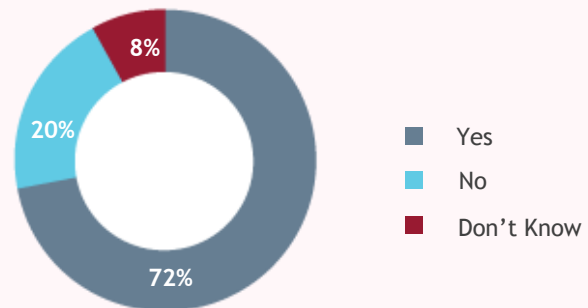
According to a survey carried out by Checkpoint in April 2020, 71% of Security Professionals reported an increase in security threats and attacks. Almost 61% of the professionals said they were concerned about the security risks of changes made to the existing networks to enable WFH. Another survey carried out in December 2020 stated that 58% of professionals reported that attacks have increased since the beginning of the pandemic.

Additionally, since employees moved from a LAN setting to VPN, an organisation's threat landscape opened new doors to attacks such as compromising VPN servers, exploits, and many more.

Phishing has always been a pain point for organisations. During the pandemic, cybercriminals used it to their advantage and developed campaigns around this theme to lure more victims. Almost 55% of the links in phishing attempts claimed helpful information on COVID-19, such as information on vaccines, masks, use of hand sanitizer, shortage of supplies, etc.

Spear Phishing attacks have increasingly switched to COVID-19 themed lures for phishing and exploiting employee's concerns over the pandemic and their

HAS YOUR ORGANISATION FACED A CYBERATTACK DURING THE PERIOD ENSUING THE SPREAD OF COVID-19 ?



loved one's safety. Cybercriminals have also shifted gears in the pandemic as the exploitation of unpatched VPN servers was one of the top methods to gain organization-wide access. A massive number of VPN products were found vulnerable. However, according to the DHS, CVE-2019-19781 and 2019-11510 remained exploited by the attackers.

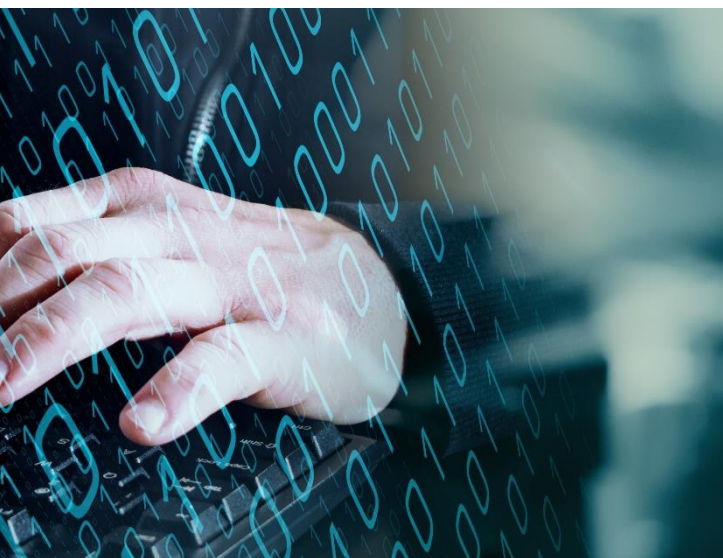
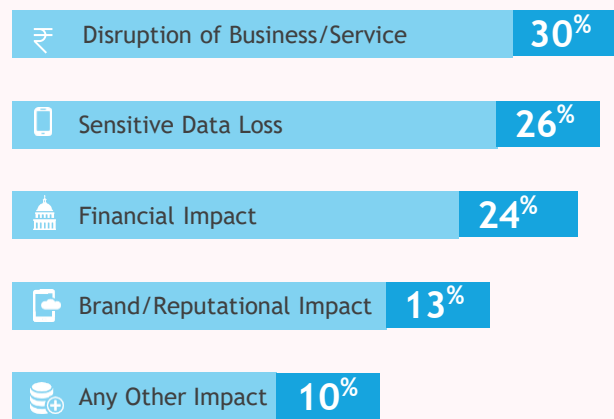


About 30% of the cyberattacks have impacted disruption of businesses and services of the organisation, with 26% resulting in loss of sensitive/ confidential data. 24% of the respondents agree that cyberattacks have impacted their organisation's financial standing.

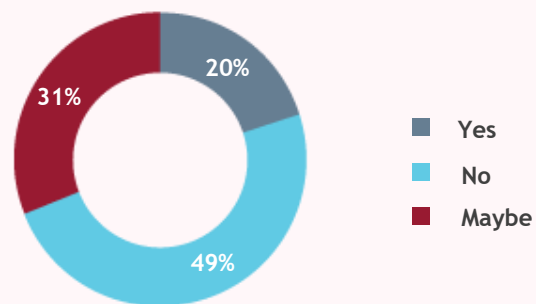
With individuals and businesses worldwide becoming more reliant on video conferencing, further aided with platforms like Skype, Microsoft Teams, Zoom, etc. the number of application-centric phishing attempts have increased as well. A typical attack begins with an impersonated mail from the platform such as Zoom or others letting the employee know that he/she has missed a meeting and the recording is available to download for a specific period. Unaware and fear struck employees usually click the link and follow the instructions that typically end up in harvesting of his/her zoom credentials or installing a backdoor on the computer system.

Around 49% of the respondents shared that they did not face any phishing attacks while 20% confirmed that their organisations witnessed phishing attacks during the period ensuing the spread of the pandemic. However, 31% of the respondents were not aware of any phishing attacks on their organisations, owing to the fact that there was no proactive monitoring to check for such attacks on their networks.

IF YOUR ORGANISATION FACED A CYBERATTACK DURING THIS TIME, WHAT WAS THE IMPACT(S) ?



DURING THIS TIME, HAS YOUR ORGANISATION AND/ OR ITS EMPLOYEES FACED A SUCCESSFUL PHISHING ATTACK ?



While COVID-19 crashed multiple markets and disrupted businesses worldwide, it flourished the sales on the dark web. Hackers put up on sale confidential data from various organisations on the dark web, including 500,000 stolen Zoom Accounts.

Sodinokibi was one of the top ransomwares used by cybercriminals during the pandemic. Sodinokibi deploys an asymmetric key scheduling algorithm that removes the need for a command-and-control server, hence, making decryption close to impossible. Proactive organisations who record their traffic have a better chance of recovering the ransomware keys when the key is sent back to the attacker. Sodinokibi removed that dependency and proved much more lethal. According to a report, innovative techniques such as the one used by Sodinokibi accounted for ransomware being the topmost security concern of 2020.

While we battled the pandemic and cybercrime together, new learnings were revealed:

- ◆ Data Security is important whether the data is at rest or in use. Encryption of sensitive data can limit a breach impact as it wouldn't be usable.
- ◆ Keep looking for ransomware, they usually land up in the inbox.
- ◆ Software must be updated, especially VPN server software and others that are the backbone of work from home culture.
- ◆ Cybersecurity awareness for employees is important, especially as the attack surface is much broader now.
- ◆ Encourage Red team exercises/ assumed breach simulations or wargaming exercises to stay prepared for the attacks.
- ◆ Be ready with an incident response plan and ensure forensic readiness.
- ◆ Avoid using social media on work laptops.
- ◆ Avoid clicking unknown links and downloads.

ENTERPRISE RISK MANAGEMENT



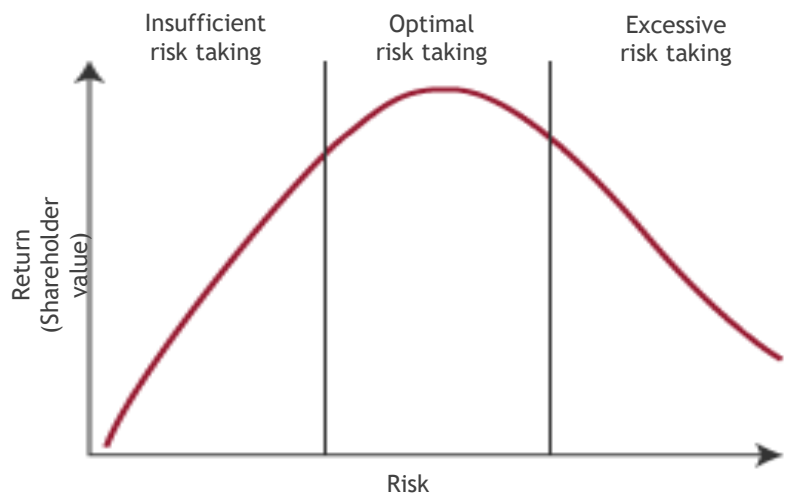
SAUMIL G SHAH
 Partner / Cyber Security
 Business Advisory Services
 BDO in India

Enterprise Risk Management (ERM) in business includes an organisation’s methods and processes adopted to manage risks and seize opportunities related to achieving their objectives.

BALANCING RISK & RETURN

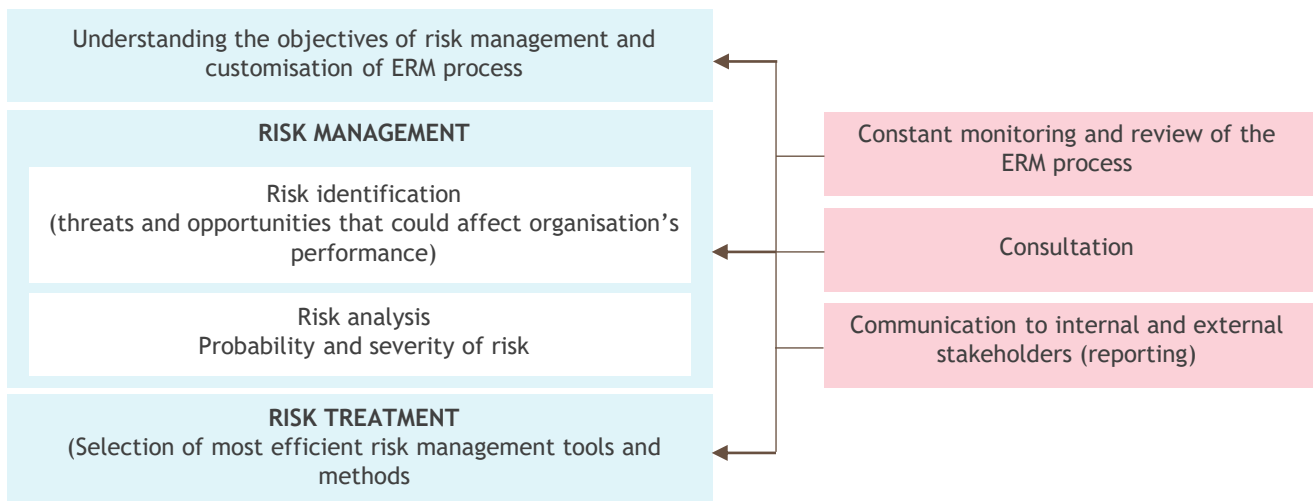
Businesses need to take various risks to create value and hence need to ensure they identify the right risks and that they are appropriately managed. Well defined ERM helps to improve the capability and coordination to manage these risks effectively.

Organizations focus on areas where the risk taken is ‘optimal’ and the returns for the same are ‘maximum’.



Source: proactuary.com

ERM - Process



Source: Journal of Risk & Financial Management: MDPI

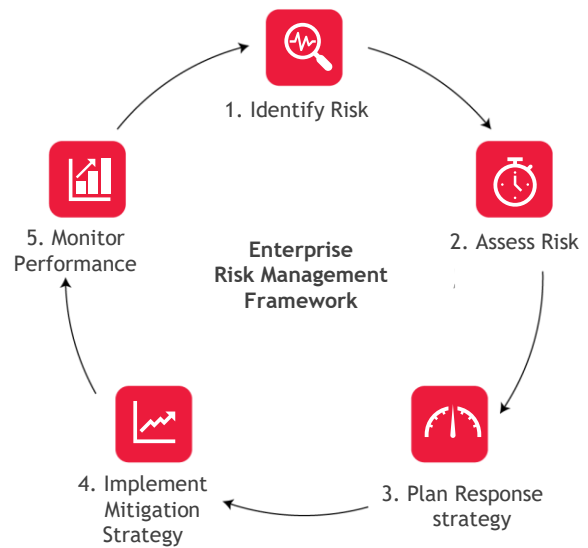
Risk management is the process of identifying and assessing the impact of the risks and planning how to respond if the risks become reality. Each and every organization should have a risk management plan. The requirement of risk management is necessary as it will help to secure the information and data and if it gets in contact with any threat then it will not affect the organization’s data.

ERM FRAMEWORK - THE NEED TO EVOLVE

ERM is not a one-time process where the risks are identified, monitored, and managed by placing controls. Examples such as COVID Pandemic and increased cyber-attacks have made organizations understand that ERM is a broad spectrum and should evolve more often to ensure that while risks are appropriately managed the needs of various stakeholders are also addressed.

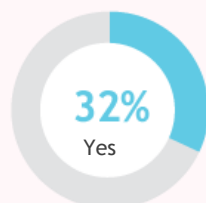
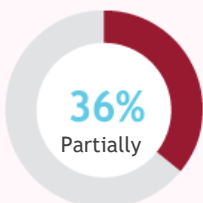
Pandemic risk has been recognized as a focus of risk management in practice; however, the COVID-19 pandemic has shown that generic pandemic risk was underestimated in both extent and proportion. COVID-19 has shown that pandemic consequences are difficult to reliably estimate, and the persistence is difficult to define making pandemic risk to be perceived as a severe threat to an entity’s overall strategic objectives. Since ERM is responsible to ensure Management create, preserve, and realize value, it is now important that organizations’ risk management approaches may need re-evaluation.

The unique characteristics of the COVID-19 pandemic can also be addressed using risk analysis. Commonly, the impact of analysed risk concerns the probability of risk occurrence and the severity of its consequences.

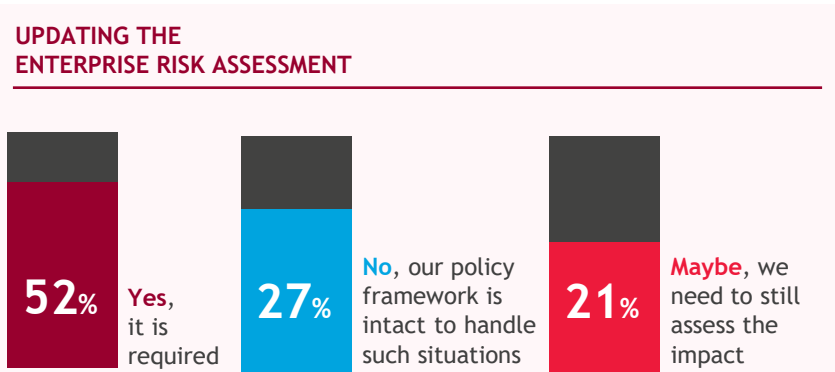


As per the survey conducted, the results highlighted 32% of the respondents claim that their ERM framework covers risks like COVID-19 pandemics, whereas 32% to 36% agree that their ERM framework neither obscures or covers such risks partially.

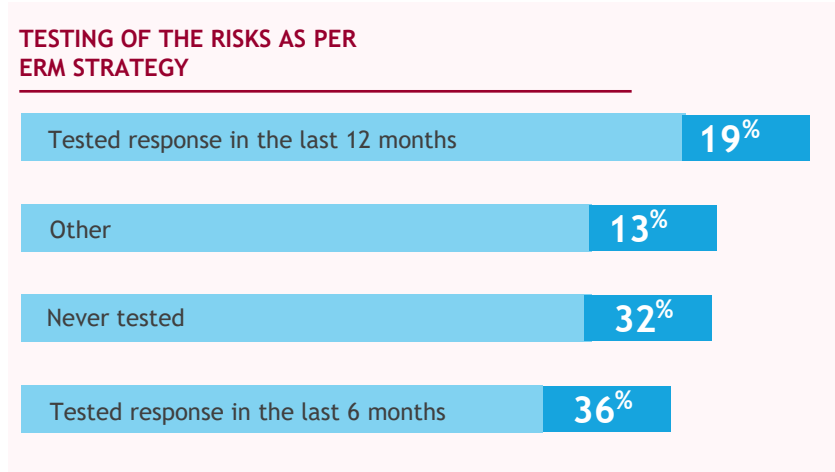
DOES YOUR RISK MANAGEMENT FRAMEWORK COVER COVID-19 RISKS ?



Owing to the above results it was also surveyed that if the response to coverage of COVID-19 in Risk Management was ‘yes’, then have the organisations made efforts to conduct drill based on risk management framework.



Further, 52% of the respondents shared that their organisations are considering updating their ERM frameworks to tackle the change in the technology landscape and remote working, enforced due to the pandemic. 21% of the respondents are yet to assess the impact of COVID-19 on their business, while 27% of the respondents are confident about their current policy frameworks that do not require updates for any such situations.



CONCLUSION

In the risk identification and risk analysis dimension, there is a need to address the ability to understand and manage pandemics as a tail event and develop reasonable scenarios for dealing with these types of risk events in the future. Future research endeavours should address the challenges within the available risk response strategies to COVID-19 disruptions and the emergence and applicability of new risk management methods.

For many companies, ERM has become an essential activity during the decade of economic growth, but the pandemic demonstrates the need for attention and rigor. The key to effectively managing ERM is to ensure that business executives/ leaders evaluate and define the enterprise risk appetite. ERM can assign risk ownership at the highest level of organisational decision making.

This opinion clarifies and formalises the enterprise’s position that certain risks, such as a pandemic, are threats to strategic goals such as business growth. Leaders can then agree in advance that however unthreatening a risk might seem, its emergence will trigger decisive and quick action to mitigate the effects – driven by a predetermined team of owners and executors.

CYBER STRATEGY FOR THE FUTURE



MUBIN SHAIKH

Partner & Leader / Cyber Security
Business Advisory Services
BDO in India

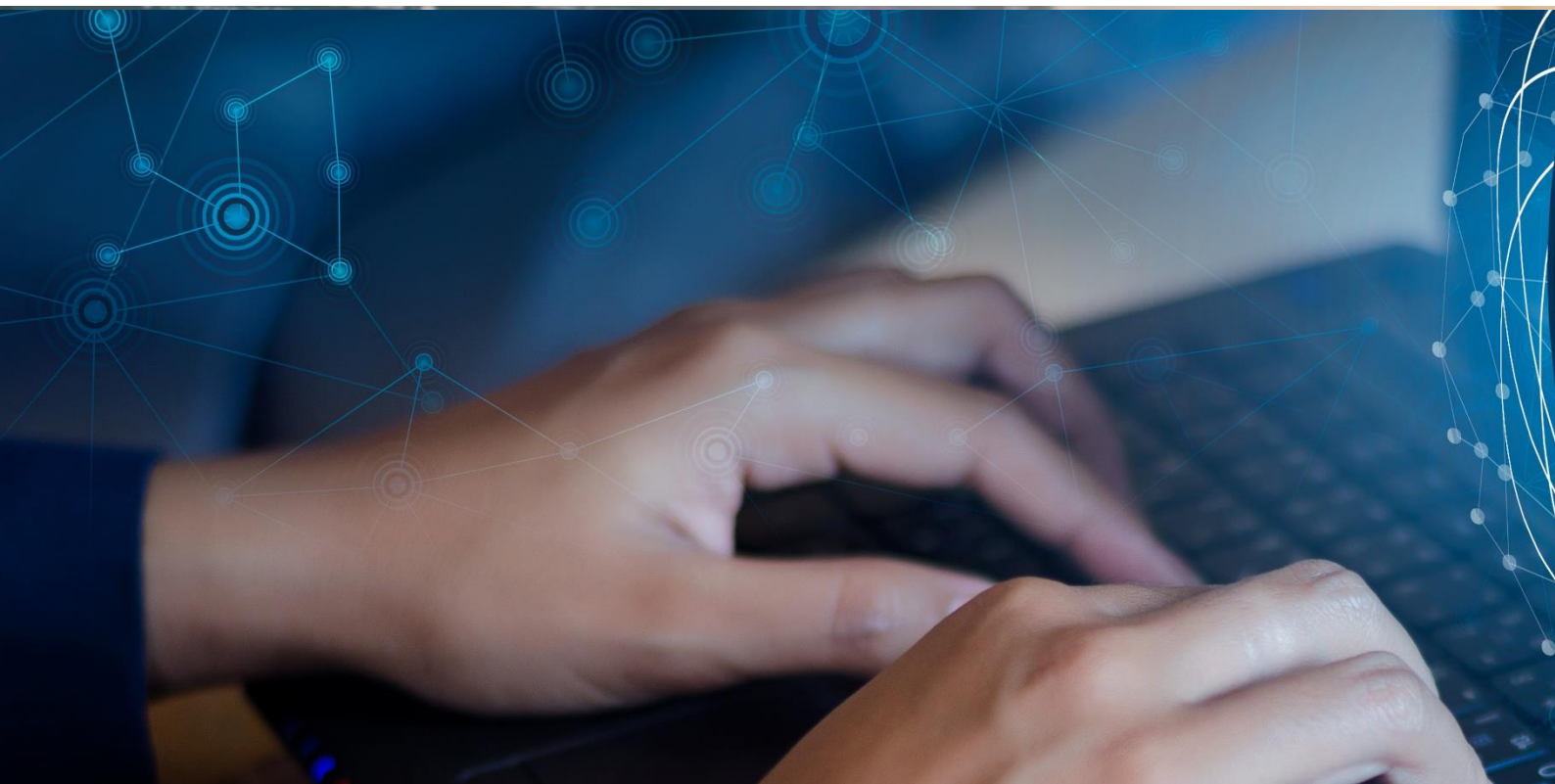
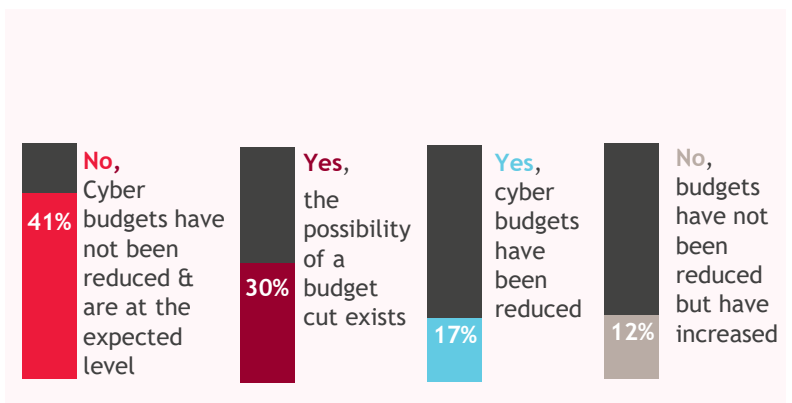
THE CYBERSECURITY LANDSCAPE IN THE PAST

Due to the use of more sophisticated techniques and strategies to hack into the IT infrastructure and gain unauthorised access to critical data, cyber professionals are devising new and more efficient capabilities to tackle this concern. In 2010, many organisations started recruiting cybersecurity professionals to identify and analyse cyber threats and related risks to mitigate or reduce them to a considerable amount. The organisations also adopted new technologies to ensure their information remained safe and secure.

Since the past few decades, attackers have always kept an eye out for an organisation's sensitive and critical information. Irrespective of the nature or motivation behind the attack, critical assets get compromised and breached, causing a substantial financial and reputational loss for the company. The Board of Directors and the management have never been so prompt in addressing the cybersecurity issues than the current times. Cybersecurity spending and budget allocations for the same had always taken a back seat due to the lack of awareness regarding the importance of safeguarding sensitive information. As per our

study, during the pandemic and due to the economic slowdown, cybersecurity budgets might have changed for most organisations.

Around 41% responded shared that they did not witness any change in cybersecurity budgets and around 12% confirmed that their budgets were increased during the given period. However, around 47% of the respondents shared that they witnessed/ possibly could witness reduction in budgets for cybersecurity, which is concerning given the rising number of attacks.

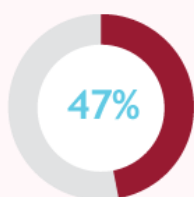


With time, the number of cyberattacks have increased across the globe. This has urged organisations to invest more in implementing cybersecurity controls to avoid data breaches and network compromise. From appointing a CISO or an information security officer to implementing technical controls to conducting information security awareness workshops for all employees or to developing customised risk management strategies, organisations are leaving no stones unturned to strengthen their overall cyber posture. The current situation has compelled most organisations to implement many new technology solutions to ensure business continuity without undertaking risk assessments for situations such as remote working for all, use of a non-standard end-point device (laptop/mobile/desktop), opening of enterprise applications to the external world. As per the study conducted 47% of the respondents believe that the overall cybersecurity posture of their organisation has reduced, increasing their risks of cyberattacks.

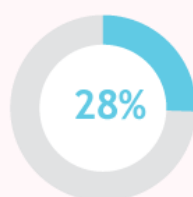
While 28% were assured that their cybersecurity postures are strong. The study gave a fair idea that 25% of the surveyed organisations never evaluated their cybersecurity postures to understand the real impact and risks.

According to a survey conducted by Black Hat, in the USA, in 2019, 65% of the organisations were expected to respond to a significant breach in one year, and 75% of security leaders were anticipating a critical infrastructure breach due to the attack. According to the Merill Research for Radware, the average cost to recover from a cyberattack for organisations with more than USD 1 billion in revenue was USD 4.6 million. The global cybersecurity market is known to increase to USD 270 billion by 2026 from USD 173 billion in 2020.

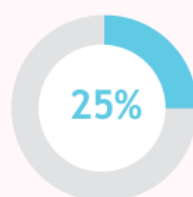
CYBERSECURITY POSTURE



Yes



No



Don't know





‘Ethical hacking’ a new term that evolved and eventually became more prominent, is known to find vulnerabilities in a computer system. In 2010, a notorious nation-state attack, Operation Aurora, was launched by Chinese military hackers on more than 20 leading technology companies. It was first made public when the internet buzzed about the compromised companies’ intellectual property.

“

In April 2011, Sony Corporation announced, hackers stole information from 77 million users of Sony PlayStation.

This breach of information at Sony Corporation included gamers’ username, password, birthdate, security question answers, and more. It took several days to recover the system and remediate the attack.

”

While Man in the middle, Social engineering, and DDoS attacks are becoming more prevalent, Crypto-jacking is an emerging online threat that involves malicious crypto mining by cybercriminals, who manage to hack both business and personal computers, laptops, and mobile devices to install malicious software. In 2018, Coinhive was a popular cryptocurrency mining service considered by leading security firms as one of the top malicious threats to any web user. The computer code of Coinhive could be used on hacked websites to steal the processing power of the visitors’ device. For fifteen months, cybercriminals used malicious programs to infect millions of devices.

The past decade has seen a drastic change in the number of cyberattacks and the ways hackers intrude into networks. In early 2017, Europol’s Serious Organized Crime Threat Assessment found that hackers were motivated by financial gain and ideological motivation. The ‘Crime as a Service’ model has often uplifted these hacker’s spirits, thereby increasing the number of attacks. While in 2016, Intel Security logged 124 different ransomware variants, a South Korean firm disclosed the enormous ransom payment - USD 01 million. This serves as a critical example for all organisations to adopt cyber strategies that fit their size and type and implement them regularly.

The Indian government data shows that in 2019 alone, there were 3.94 lakh instances of data breach. According to the Indian Computer Emergency Response Team (CERT-In), 336 websites belonging to central ministries were compromised in 2019.



LIKELIHOOD AND IMPACT OF CYBERATTACKS OVER THE NEXT FEW YEARS

A successful cyberattack can cause considerable damage to an organisation. Across the globe, the repercussions of the pandemic have given rise to several cybercrimes leading to data loss and increased financial concerns. According to the National Cyber Security Coordinator, India was hit by 375 cyberattacks daily with four lakh malware counts in 2020. Haldiram's a very well-known food manufacturing company based out of India for more than eight decades, faced a ransomware attack on its servers, with a ransom demand of USD 7,50,000. In May 2020, 4.75 crores of Truecaller's Indian user data were sold on the dark web. In August 2020, researchers at Comparitech discovered a database with 235 million Instagram, TikTok, and Youtube user profiles online.

Due to the use of highly sophisticated techniques by the attackers, it becomes essential for organisation to adopt new cutting-edge technologies to safeguard their critical infrastructure. Artificial Intelligence (AI), will help analyse and break into secure systems faster than any human and disrupt a significantly larger IT network scale. Another emerging technology - Blockchain, can prevent disruptions caused and secure critical infrastructure. Cyberattacks are likely to become more common over the coming years, and we will see a full-scale cyber warfare level event in this decade.

HOW A WELL-STRUCTURED CYBER STRATEGY CAN HELP IN SECURING AN ORGANISATION'S FUTURE CYBER POSTURE

In times of digital transformation, cybersecurity has become vital for any organisation to smoothen their businesses' operation and avoid more significant impacts caused due to the cyberattacks. As per the survey, 32% of the respondents have requested for a cybersecurity review, while 38% have proactively performed one during the pandemic.

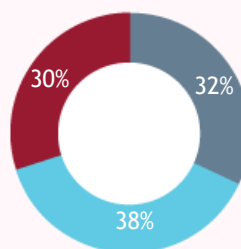


AI in the cybersecurity market is projected to generate a revenue of USD 101.8 billion in 2030. Increasing from USD 8.6 billion in 2019, progressing at a 25.7 % CARG during 2020-2030.



One size does not fit all, and hence every organisation should have its unique strategy or plan to secure their data and critical infrastructure.

CYBERSECURITY REVIEWS IN COVID-19 PANDEMIC



- Yes, requested a cybersecurity review
- Already performed cybersecurity review
- No, not yet requested a cybersecurity review

CYBER STRATEGY IS BROADLY BASED ON FOUR MAIN PILLARS

- ▶ **SECTORIAL REQUIREMENTS**
- ▶ **BUSINESS REQUIREMENTS**
- ▶ **REGULATORY REQUIREMENTS**
- ▶ **CYBERSECURITY AS AN EDGE TO BUSINESS**

Sectorial Requirements

Various industrial sectors adopt international standards and guidelines to abide by the law and maintain a robust infrastructure. The standard remains typical for all industries. The controls implemented differ greatly depending on the type of organisation. E.g., controls implemented for a pharmaceutical company under ISO/IEC 27002:2013 will highly differ from the controls implemented for any organisation in the BFSI sector.

Business Requirements

Depending on an organisation's size and type, they should use cutting-edge emerging technology and strengthen their cyber strategy. Based on the survey conducted, it was noted that only 20% of firms have a cyber insurance policy, while 80% are either planning to invest in one or don't feel a need to do so. Cyber insurance is a way forward in safeguarding all critical assets for organisations of all sizes and types. Setting out clear ownership and responsibilities will also help in designing and following the cyber strategy religiously. Most businesses are likely to experience significant disruption to their business-as-usual operations and face business underperformance throughout the COVID-19 crisis.

CYBER INSURANCE



37%

cyber-insurance available in the market is still at a nascent stage and may not serve our purpose



22%

No, cyber-insurance is not a part of our strategy of cyber risk transfer



21%

Yes, we will buy cyber-insurance immediately



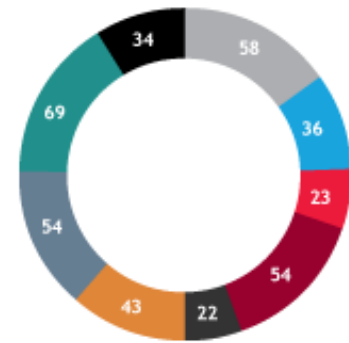
20%

Yes, we already have cyber-insurance

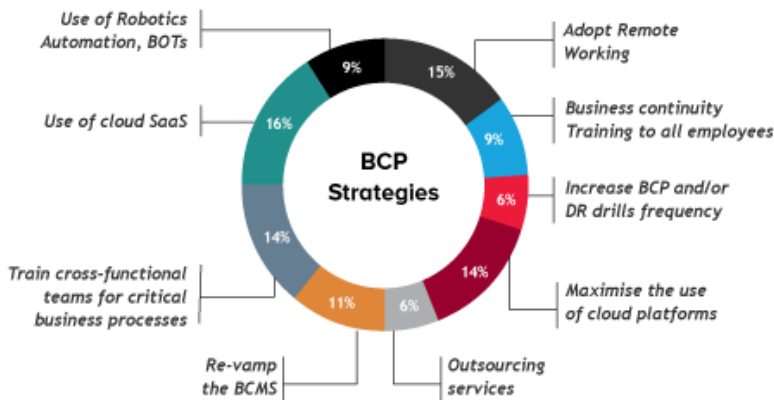
Regulatory Requirements

These are mainly based on the cybersecurity requirements set for compliance by various regulatory bodies. The guidelines set out by the RBI, SEBI, FDA, and others help in peer benchmarking in the industry. It sets out clear goals to build a cyber strategy and increases the competition to tighten its overall cybersecurity posture. Regulatory requirements enforce business to have continuity plans and invest in technologies for business continuity. In our survey, we asked respondents if they were to ensure business continuity with technology in a similar situation in the future, which strategies would they use. Out of the total respondents, many opted for business continuity trainings and cloud platforms.

Use Of Technology In Business Continuity



BCP Strategies



- Adopt remote working
- Business Continuity training to all employees
- Increase BCP and/or DR drills frequency and seriousness
- Maximise the use of cloud platforms to host enterprise applications and infrastructure
- Outsource as much as possible and blind vendors to provide services during future crises
- Re-vamp the business continuity plan (BCP)/management system

CYBERSECURITY AS AN EDGE TO BUSINESS

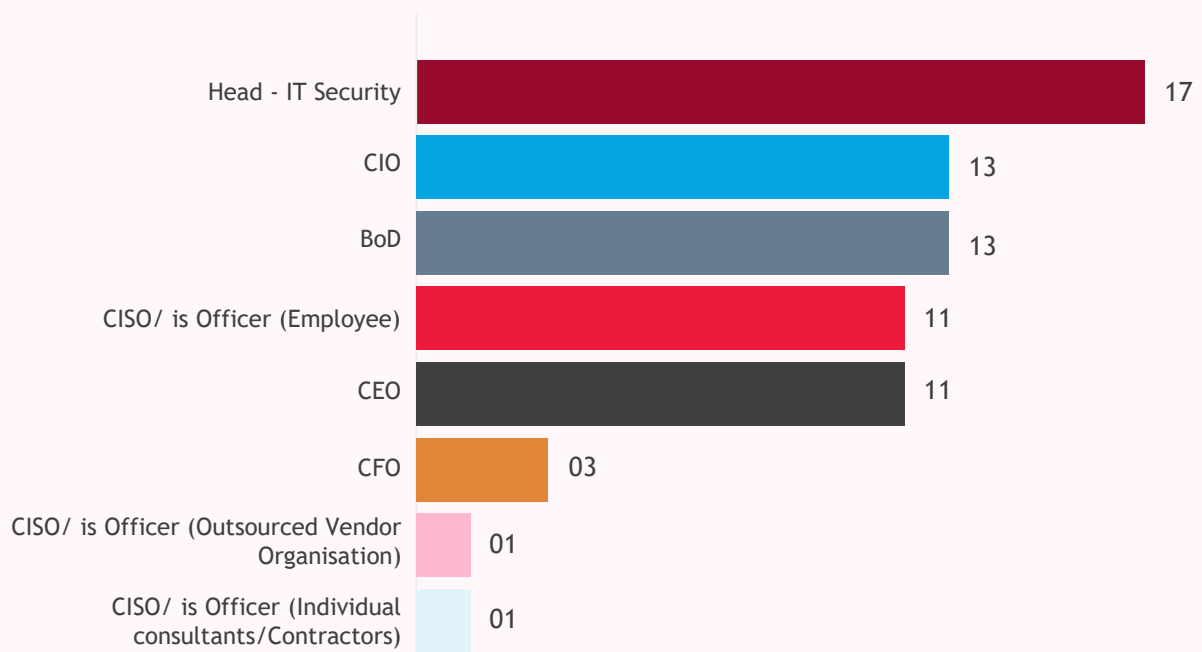
Based on the survey, it is evident that emerging technologies such as AI are currently booming and will continue at a faster rate, aiding the operations to run smoothly and giving an edge to businesses adopting these technologies. Regular security testing and adhering to the existing policies and procedures can help devise a robust cyber strategy. However, it is required that budget approvals for technologies are required. As per the survey the COVID-19 situation has still not changed the approval process for cybersecurity technology and services.



WHO IN YOUR ORGANISATION IS RESPONSIBLE FOR CYBERSECURITY?

Through the survey and the graph below, it is evident that the respondents claim that the IT security head is responsible for any data loss or breach. The CIO and the Board of Directors are also held accountable for the damage in some cases. If a risk arises, an adequate enterprise risk management plan could mitigate the risk correctly. If this is not implemented correctly by all the employees, then the risk will damage the computer systems or data.

RESPONSIBILITY OF CYBERSECURITY



CONCLUSION

With cyberattacks increasing, every organisation should maintain and efficiently execute a risk management plan to eliminate the risks arising from these attacks. The COVID-19 outbreak and the ensuing lockdowns have further increased the number of cyberattacks in 2020, which is foreseen to only increase in the future. To protect critical information and assets from such attacks, all organisations should use emerging technologies to get started on the cyber strategy journey and safeguard their critical assets and networks.

By 2030, many firms will be adopting the use of AI to save their data. Cloud computing will also help to keep the data and information safe. Hence a firm should always be ready with its future strategies to deal with any threat or risk.

WAY FORWARD

Until the last decade, to safeguard an organisation's critical data, most employees across the globe worked from office set-ups and on secured data network lines. Adequate security was ensured for computer systems by deploying sophisticated technologies at workplaces. However, during the pandemic, most employees began operating from home, resulting in an increased number of cyberattacks. Huge tech giants and other large companies have already devised their future strategies for smooth and efficient working. Simultaneously, some organisations have now come to realise the importance of work from home and have seen improved results in the form of better-quality work and more significant revenues.

In contrast, certain companies still cannot operate efficiently from home, and hence their future strategy will include an office based set up. Tech giants have already devised a way in which their employees have a flexible culture and have an option of remote working permanently. At the same time, other organisations are coming up with a hybrid model where employees can partly work from home and partly from the office depending on the business requirements and the comfort of the employee.

Organisations need to quantify the revenues in terms of cyber risk and anchor all the risks through a risk appetite. The effectiveness of the risks identified should be ensured with a customised risk management strategy and a cyber roadmap that aids the company plan and achieves its future business goals.

Security challenges have undoubtedly increased since the WFH culture got widely adopted during the pandemic. A network link, shared wi-fi connection, or mobile hotspot are key reasons for increasing cyber-crimes. Worldwide, security challenges are increasing daily due to the unavailability of secured and adequate facilities to protect data from home.

Organisations are advised to build robust cyber risk postures and build smart strategies around risk management to avoid any unforeseen data breach or compromise to the network, which could affect the reputation of the firm, along with more significant financial losses and non-compliance to the regulatory requirements or compromise in the quality as compared to the reputed international standards.



ABOUT BDO GLOBAL

BDO is a leading professional services organisation with presence in 167 countries, and over 91,000 people working out of more than 1,600 offices. We deliver assurance, tax, advisory, and consulting services to clients throughout the country and around the globe.

- We offer sensible, actionable advice grounded in local knowledge backed by regional and global experience
- We set high standards and our global systems give our people responsibility for delivering tailored service that is right for clients
- We support our clients every step of the way as they expand abroad



Leading consolidation in the mid tier	Over 1,600 offices in more than 165 countries	Over 91,000 highly skilled partners and staff worldwide	BDO posted global revenues of \$10.3 billion in 2020
---------------------------------------	---	---	--

TO BE THE LEADER FOR EXCEPTIONAL CLIENT SERVICE

anticipating **client needs** and being forthright in our views to ensure the best outcome for them

ANTICIPATING CLIENT NEEDS

being clear, open & swift in our **communication**

CLEAR COMMUNICATION

agreeing to and meeting our **commitments**: we deliver what we promise, everyday, for every client

MEETING OUR COMMITMENTS

providing the right environment for our **people** and the right people for our clients

ENCOURAGING OUR PEOPLE

creating **value** through giving clients up to date ideas and valuable insight and advice that they can trust

DELIVERING VALUE

ABOUT BDO IN INDIA

BDO in India offers Strategic, Operational, Accounting and Tax & Regulatory advisory & assistance for both domestic and international organisations. We work cohesively, partnering with our clients to render continued expertise driven advisory. With a deep cultural understanding of business geography, our functional heads offer knowledge and expertise in establishing, structuring and operating business in India.



150 PARTNERS
3000 DIRECTORS
STAFF



10 KEY CITIES



Ahmedabad, Bengaluru, Chennai, Goa
 Hyderabad, Kochi, Kolkata, Mumbai
 Delhi NCR, Pune

ASSURANCE

- Accounting Advisory Services
- Financial Statement Audit and Attestation Services



BUSINESS SERVICES & OUTSOURCING

- Global Outsourcing
- Shared services & Outsourcing
- Technology Services



ADVISORY

- Business Restructuring
- Corporate Finance
- Cyber Security
- Business Analytics
- Due Diligence
- Forensics
- Government Advisory
- Resolution Advisory
- Risk and Advisory Services
- Technology & Business Transformation Solutions
- Valuations

TAX

- Corporate income tax
- Transfer pricing
- Global Employer Services
- Transaction Tax
- Regulatory and Exchange Control
- Goods & Services Tax (GST)
- Customs & International Trade
- Pre-GST Indirect Tax Assessment & Litigation Assistance
- Tax Technology



ABOUT CII

The Confederation of Indian Industry (CII) works to create and sustain an environment conducive to the development of India, partnering industry, Government and civil society, through advisory and consultative processes.

For 125 years, CII has been working on shaping India's development journey and, this year, more than ever before, it will continue to proactively transform Indian industry's engagement in national development.

CII is a non-government, not-for-profit, industry-led and industry-managed organization, with about 9100 members from the private as well as public sectors, including SMEs and MNCs, and an indirect membership of over 300,000 enterprises from 288 national and regional sectoral industry bodies.

CII charts change by working closely with Government on policy issues, interfacing with thought leaders, and enhancing efficiency, competitiveness and business opportunities for industry through a range of specialized services and strategic global linkages. It also provides a platform for consensus-building and networking on key issues. Extending its agenda beyond business, CII assists industry to identify and execute corporate citizenship programmes. Partnerships with civil society organizations carry forward corporate initiatives for integrated and inclusive development across diverse domains including affirmative action, livelihoods, diversity management, skill development, empowerment of women, and sustainable development, to name a few. With the Theme for 2020-21 as Building India for a New World: Lives, Livelihood, Growth, CII will work with Government and industry to bring back growth to the economy and mitigate the enormous human cost of the pandemic by protecting jobs and livelihoods.

With 68 offices, including 10 Centres of Excellence, in India, and 8 overseas offices in Australia, Egypt, Germany, Indonesia, Singapore, UAE, UK, and USA, as well as institutional partnerships with 394 counterpart organizations in 133 countries, CII serves as a reference point for Indian industry and the international business community.

Confederation of Indian Industry

The Mantosh Sondhi Centre

23, Institutional Area, Lodi Road, New Delhi - 110 003 (India)

T: 91 11 45771000 / 24629994-7

E: info@cii.in • W: www.cii.in

Reach us via our Membership Helpline Number: 00-91-99104 46244

CII Helpline Toll Free Number: 1800-103-1244



cii.in/facebook



cii.in/twitter



cii.in/linkedin



cii.in/youtube





ACKNOWLEDGMENT

We would like to express our appreciation to all our respondents and members of the industry for sharing their experiences, valuable inputs, and time.

Our Cyber Security team: Mubin Shaikh, Saumil G Shah, Saurabh Mehendale, Abhijeet Barve, Sanket Jalgaonkar, Khyati Shah have expert-led the analysis of this report, alongside the Marketing and Communications team: Smriti Saluja, Bhavna Balaram, Venezia Dcruz, Harsh Pandya, Praveer Trivedi for making it insightful & noteworthy for our audiences.

We would also like to extend gratitude to CII-team for their support and Sijo Rodrigues for facilitating the relationship and supporting the study through an ever-meaningful relationship with BDO in India & Confederation of Indian Industry (CII)

Contact Us

For any queries, please get in touch with our experts at cybersecurity@bdo.in

LAV GOYAL

Partner & Head
Business Advisory Services
m : +91 98 1011 4013
e : lavgoyal@bdo.in

MUBIN SHAIKH

Partner & Leader
Cyber Security
m : +91 98 8063 0062
e : mubinshaikh@bdo.in

SAUMIL G SHAH

Partner
Cyber Security
m : +91 99 0007 9563
e : saumilgshah@bdo.in

VIRENDRA SINGHI

Associate Partner
Cyber Security
m : +91 98 2008 7797
e : virendrasinghi@bdo.in

NIPUN JASWAL

Director
Cyber Security
m : +91 70 4271 1337
e : nipunjaswal@bdo.in

SAURABH MEHENDALE

Director
Cyber Security
m : +91 97 6934 6933
e : saurabhmehendale@bdo.in

For any other queries or feedback, kindly write to us at marketing@bdo.in

BDO in India offices

Ahmedabad

The First, Block C - 907
Behind ITC Narmada, Keshavbaug
Vastrapur, Ahmedabad 380015, INDIA
Tel: +91 79 6816 1600

Bengaluru

SV Tower, No. 27, Floor 4
80 Feet Road, 6th Block, Koramangala
Bengaluru 560095, INDIA
Tel: +91 80 6811 1600

Chennai

No. 443 & 445, Floor 5, Main Building
Guna Complex, Mount Road, Teynampet
Chennai 600018, INDIA
Tel: +91 44 6131 0200

Delhi NCR - Office 1

The Palm Springs Plaza, Office No.
1501-10, Sector-54, Golf Course Road
Gurugram, 122001, INDIA
Tel: +91 124 281 9000

Delhi NCR - Office 2

Windsor IT Park, Plot No: A-1
Floor 2, Tower-B, Sector-125
Noida 201301, INDIA
Tel: +91 120 684 8000

Goa

701, Kamat Towers
9, EDC Complex, Patto
Panaji, Goa 403001, INDIA
Tel: +91 832 674 1600

Hyderabad

1101/B, Manjeera Trinity Corporate
JNTU-Hitech City Road, Kukatpally
Hyderabad 500072, INDIA
Tel: +91 40 6814 2999

Kochi

XL/215 A, Krishna Kripa
Layam Road, Ernakulam
Kochi 682011, INDIA
Tel: +91 484 675 1600

Kolkata

Floor 4, Duckback House
41, Shakespeare Sarani
Kolkata 700017, INDIA
Tel: +91 33 6766 1600

Mumbai - Office 1

The Ruby, Level 9, North West Wing
Senapati Bapat Marg, Dadar (W)
Mumbai 400028, INDIA
Tel: +91 22 6277 1600

Mumbai - Office 2

601, Floor 6, Raheja Titanium
Western Express Highway, Geetanjali
Railway Colony, Ram Nagar, Goregaon (E)
Mumbai 400063, INDIA
Tel: +91 22 6831 1600

Pune - Office 1

Floor 6, Building # 1
Cerebrum IT Park, Kalyani Nagar
Pune 411014, INDIA
Tel: +91 20 6763 3400

Pune - Office 2

Floor 2 & 4, Mantri Sterling, Deep
Bungalow Chowk, Model Colony
Shivaji Nagar, Pune 411016, INDIA
Tel: +91 20 6723 3800

Ahmedabad

Bengaluru

Chennai

Goa

Hyderabad

Kochi

Kolkata

Mumbai

New Delhi

Pune

Note: The information contained herein has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The information cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO India LLP to discuss these matters in the context of your particular circumstances. BDO India LLP and each BDO member firm in India, their partners and/or directors, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO India LLP, a limited liability partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the international BDO network and for each of the BDO Member Firms.

Copyright ©2021 BDO India LLP. All rights reserved.

Visit us at www.bdo.in

