Opinion | Pg 14

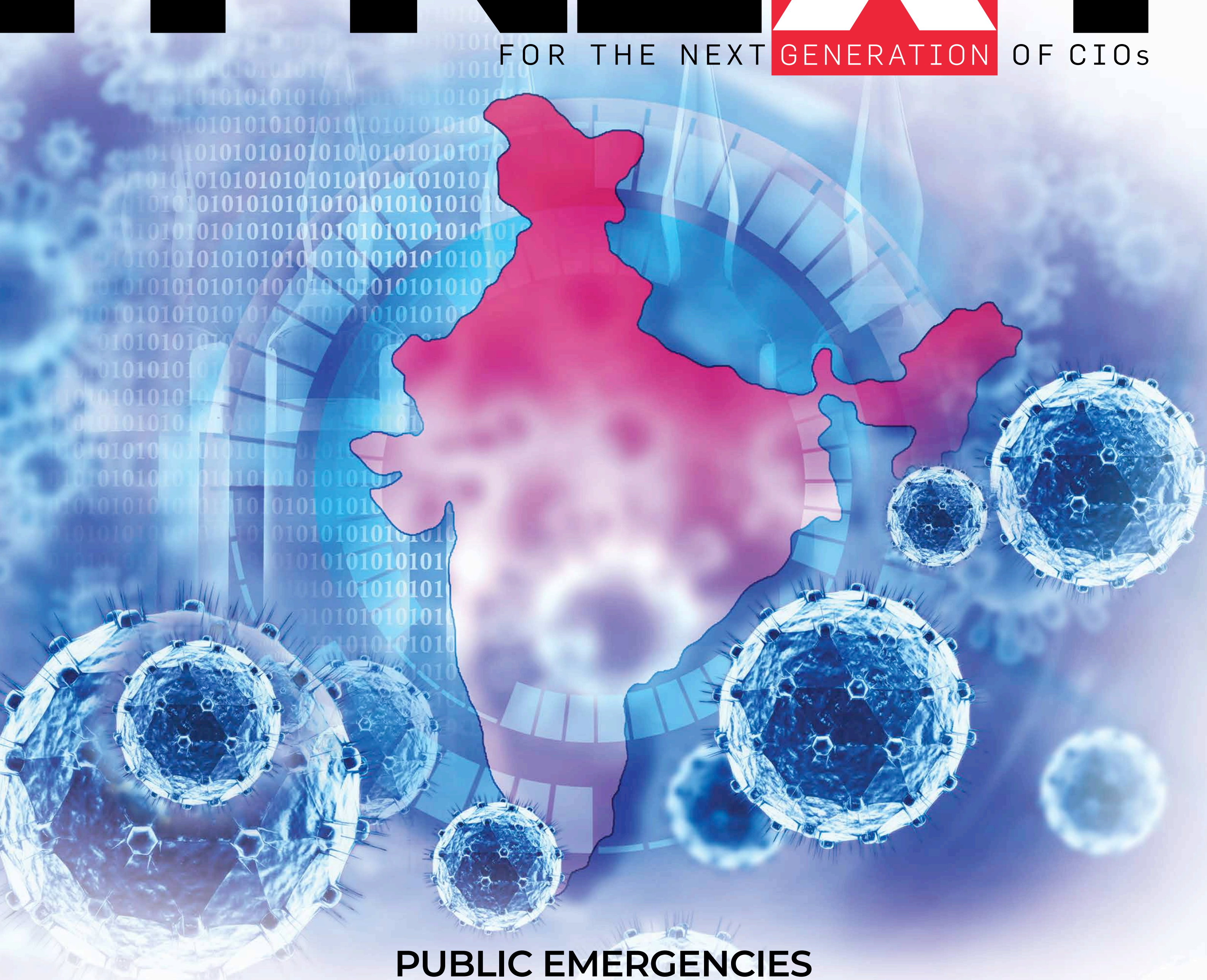
FinTech Start-Ups Are Going To Be The Next Big Employment Creators

Insight | Pg 18

The Rise And Rise Of Big Breaches

IT NEXT

FOR THE NEXT GENERATION OF CIOs



PUBLIC EMERGENCIES

How tech can help...

The COVID-19 crisis has exposed many gaps in our management of large-scale public emergencies. An integrated approach to healthcare digitization can help us prepare better for the future.

May 2021 | ₹100 | Volume 12 | Issue 02 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

Tech could really help. But we need leadership.

We saw techies quickly putting together useful apps and resources for patients and relatives, which helped immensely, at a time when the disaster was on the verge of going completely out of control. Imagine if we had done all that a little earlier and in a little more organized and coordinated manner!

Shyamanuja Das

The kind of trauma we have gone through in the wake of second wave of COVID will forever remain in our memory. Waking up every morning to find friends, relatives, and acquaintances succumbing to the disease is something that would be difficult to forget. The fact that many of them died while waiting for Oxygen or medicine or bed – or a combination thereof – means it was not just grief, but an added sense of guilt and dejection that we went through.

Not all these could have been prevented perhaps, but surely it could have been drastically reduced, if only we had planned a little better. Consider this. It was not that Oxygen was not available. Industrial Oxygen was available in plenty in states like Odisha, Jharkhand, and Chhattisgarh. They just needed to be converted to Medical Oxygen and had to be transported to the places where people needed them—like in Delhi, UP, Gujarat and Maharashtra. Oxygen came. But for many, it was too late.

We keep talking of digital technologies closing the gap between demand and supply in the most efficient manner. When was it needed more than in such situations? What can be more valuable than human lives?

A timely and proper intervention of technology could have even prevented so many casualties, just by predicting well. A little bit of not-so-cutting-edge technology could have ensured that a patient scrambling to get a bed in a hospital throughout the city could have been avoided. A lot of the severe cases could have been prevented with timely medical help through videoconferencing at their homes.

In short, the impact of this disaster could have been drastically minimized, if we had thought about applying technology proactively. We saw techies quickly putting together useful apps and resources for patients and relatives, which helped immensely, at a time when it was on the verge of going completely out of control. Imagine if we had done all that a little earlier and in a little more organized and coordinated manner!

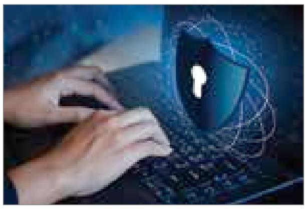
We have no dearth of technology manpower in India. We have no dearth of ideas. All we need is putting them together effectively and providing leadership. CIOs, with their track record of translating problems to definite technology solutions, can fill that void of leadership.

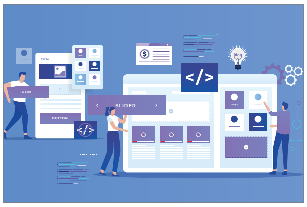
With that thought in mind, we invited a few CIOs to deliberate on how to do it better next time—not just of managing public emergencies like this, but in preventing them as well. A lot of great ideas came with a keen desire to work together for the cause.

The cover story this time captures some of these thoughts and actionable items. ■

MAY 2021
VOLUME 12 | ISSUE 02

Content





Cover Design:
ANIL VK

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

MANAGEMENT
Managing Director: Dr Pramath Raj Sinha
Printer & Publisher: Vikas Gupta

EDITORIAL
Editorial Director: Shyamanuja Das
Assistant Manager - Content: Dipanjan Mitra

DESIGN
Sr. Art Directors: Anil VK, Shokeen Saifi
Associate Art Director: Shri Hari Tiwari
Sr. Visualiser: Baiju NV

SALES & MARKETING
Executive Director - B2B Tech:
Sachin Nandkishor Mhashilkar (+91 99203 48755)
Associate Publisher & Director - Community:
Mahantesh Godi (+91 98804 36623)
Associate Director - Enterprise Technology:
Vandana Chauhan (+91 99589 84581)
Head - Community Engagement:
Vivek Pandey (+91 9871498703)
Head - Community - NEXT100 & CIOs:
Megha Bhardwaj
Community Manager - B2B Tech: Renuka Deopa
Senior Manager - Community Development:
Neelam Adhangale

Regional Sales Managers
South: BN Raghavendra (+91 98453 81683)
West: Shankar Adaviyar (+91 9323998881)
Ad Co-ordination/Scheduling: Kishan Singh

PRODUCTION & LOGISTICS
Manager - Operations: Rakesh Upadhyay
Asst. Manager - Logistics: Vijay Menon
Executive - Logistics: Nilesh Shiravadekar
Logistics: MP Singh & Mohd. Ansari
Head - Digital & Event Operations: Naveen Kumar

OFFICE ADDRESS
9.9 Group Pvt. Ltd.
(Formerly known as Nine Dot Nine
Mediaworx Pvt. Ltd.)
121, Patparganj, Mayur Vihar, Phase - I
Near Mandir Masjid, Delhi-110091
Published, Printed and Owned by 9.9 Group Pvt. Ltd. (Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.) Published and printed on their behalf by Vikas Gupta. Published at 121, Patparganj, Mayur Vihar, Phase - I, Near Mandir Masjid, Delhi-110091, India. Printed at Tara Art Printers Pvt Ltd., A-46-47, Sector-5, NOIDA (U.P.) 201301.

Editor: Vikas Gupta

9.9 GROUP

Love For 'The Gentleman's Game'

NEXT100 winner 2018 **Ashutosh Dhawan,** Platform Lead: R&D IT, Syngenta Services, shares his immense passion and love for cricket and how it has helped him both personally and professionally...

And the game goes on...love for cricket keeps the spirit high and teaches many lessons

It is a well known fact that Indians and their love for cricket go hand in hand. It's not just any other sport for us, it's a religion. Youngsters with their bats and balls at every nook and corner of the country is a common sight.

My passion for cricket dates back from the time when I was just five. I used to play with my elder brother in our house which had big verandah right in the middle. Then I started going to playgrounds and practiced over the weekends. This gave me the confidence to start taking part in various tournaments. I also captained the school cricket team. And, I still feel so elated when I tell people that I was the opening fast bowler of the team and used to swing the new ball. The ball was bought by pooling Rs 10 each and was also the winning prize of the match. As I grew up, playing cricket took a backseat and watching cricket took the front seat. I used to watch all formats of the game. But, One Day cricket was my one true love. With the introduction of the IPL, T20 format of the game is my one true eternal love now.

Playing cricket made a comeback to my life once again when I moved to Pune in 2014 and joined Syngenta Services. I joined Team Synergy, which is the employee engagement team at Syngenta and the lead sports group. It has been seven years now and I have organized four cricket, two football, two badminton and three table tennis tournaments. I also play cricket over the weekend in my society.

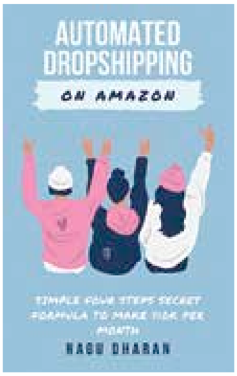
Cricket has not only helped me feel healthy, fit and strong but also made me feel confident and proud of who I am. It has helped me understand the importance of putting team above an individual. It has also taught me how to handle failures. ■

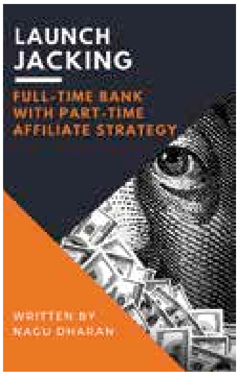
As told to Dipanjan Mitra, Team ITNEXT

Ashutosh Dhawan *Snapshot*

Ashutosh Dhawan is Platform Lead: R&D IT at Syngenta Services. He has been a NEXT100 winner in 2018. Earlier, he had served in esteemed companies like Mphasis, Prospecta Software, Nokia Siemens Networks, SAP Labs India, etc. Dhawan completed his MCA from Kurukshetra University and BSc in Computer Science from Dyal Singh College.

SIMPLE 4 STEPS
SECRET FORMULA TO EARN $10K MONTH
The New Online Business Blueprint with step-by-step walkthrough
Cheatsheets to track your progress
COMPILED BY NAGU DHARAN





The Free Video Course on Email Marketing...
HELLO
WELCOME
&
WATCH THIS
VIDEO FIRST
The Easy Strategy To Get Success In Affiliate Marketing...

Learn & Earn Digitally

How to best use your spare time and earn money, lessons from a veteran

NEXT100 winner 2019 **Nagendran Ponnan,** DGM - IT, Ramco Cements, shares his immense passion for internet marketing and ways of earning online...

Internet marketing is my passion or indulgence. So, I am continuously investing a lot of my spare time and money to learn more about it. Also, I learned a lot of things from internet marketing. Now I have turned to teach the things I learned to people over various medium of the internet, such as Kindle books, Audiobooks, YouTube videos, and blogging.

My usual work in my spare time is finding a good internet marketing course and learning new things. Then, I compile everything that I learned on my website, and talk about the product as a review on my private YouTube channel. Also, I create a video course about these learnings. I'm also constantly learning to promote my stuff over the internet with both free traffic and paid traffic methods.

In my own interest, I learned Google PPC ads, YouTube ads, Display ads, Facebook lead ads, etc. Also, periodically I spent money on these networks to promote my own stuff. Over the period of my learning, I gained experience in affiliate marketing, email marketing, solo ads, paid ads, sales funnels, etc.

I want to give a free tip for anyone who wants to earn money online. There are many ways to earn money online. By using both blackhat and whitehat methods, you can earn. With the blackhat method, you may earn money quickly. But at the same time, you will lose quickly. So, always the whitehat method is a good option. One of the best whitehat methods is email marketing.

With email marketing, you need to build your email list by giving away any gift. This gift can be anything, such as ebook, video, free report, etc. It should give some value to your leads. To collect and add email ids to your list, you need to have an opt-in page or landing page autoresponder service. So, people who visited your landing page will provide their email to get your free value gift. Then the email will be stored in your autoresponder service, where you can schedule follow-up emails that promote any of the products you want to sell to them.

At the same time, your visitors will get the gift automatically once they have given their email id on your landing page. In this way, you collect many people's email ids and follow your offers via autoresponder. This is one of the legitimate ways to earn money online. ■

As told to Dipanjan Mitra, Team ITNEXT

Nagendran Ponnan

Snapshot

Nagendran Ponnan is DGM - IT at Ramco Cements. He has been a NEXT100 winner in 2019. Earlier, he was associated with companies, such as LYNK Logistics and Balenz. He completed his MCA from PSR Engineering College.

PUBLIC EMERGENCIES

How tech can help...

The COVID-19 crisis has exposed many gaps in our management of large-scale public emergencies. An integrated approach to healthcare digitization can help us prepare better for the future.

By Jatinder Singh

The explosive resurgence of Coronavirus cases across India has put a severe strain on our healthcare management system. The second wave of the pandemic has flagged our frail emergency response readiness and inapt health infrastructure.

The scenes of myriad funeral pyres and desperate appeals from people to save them and their loved one's lives are becoming national and global headlines. Amidst a frightening shortage of medical oxygen, medicines, vaccines, and intensive care units in hospitals, India has also dealt with the deluge of misinformation circulated through several social media channels around COVID conspiracies, treatment, and risks.

These events have exacerbated the COVID-19 situation in the world's second-most populous nation, intensifying fear, anxiety, despair, and uncertainty among people.

The ferocity of the second wave was such that many people, due to the shortage of antiviral drugs and medicines in the open market, turned to profit-gougers to buy for a 10-20 times higher price than the government-approved rate. With over 2.67 crore COVID cases and increasing, this unparalleled public health emergency has stunned India and broke the confidence of its public health experts.

These tumultuous times have set alarm bells ringing in the power corridors, and the call for a rapid transformation in healthcare and public safety management has become louder than ever. Many countries worldwide have demonstrated how, by leveraging data, conventional tech, and new-age tech solutions, they can detect the virus carriers early, break the chain of infections and accelerate vaccine development.

During the last fourteen to fifteen months, we've experienced the role played by technologies to help us working from home, virtually interacting with people, attending schools and colleges, ordering groceries, and several other things. Now, the time is to replicate those technological interventions to advance the public emergency response and address healthcare skill gaps in India.

How can we prepare ourselves better?

It is possible to minimize the severity of any crisis provided there are the right resources and solutions available to take early and decisive steps. Even before the Coronavirus pandemic hit us last year, many health professionals and industry experts had posited the possibility of a global threat from unknown infectious diseases. After the first wave of COVID, epidemiologists had warned about the possible surge of cases in the country. However, India failed to take concrete prevention steps.

In any public healthcare emergency, the key factors that play a pivotal role are: timely prediction, hands-on public warning mechanism, effective control management, strong coordination between states and central government agencies, emergency response strategy, and action plan readiness. India struggled to implement any of these necessary steps promptly.

The biggest reason for India's failure to predict the unprecedented rise of Coronavirus cases was the unscientific way it adopted to lift pandemic restrictions prematurely due to the delusion

> **Whatever data is available today, that should be made available to the national agencies. For instance, why can't the individual reports of RT-PCR, the test to detect severe acute respiratory syndrome, go into a central repository? Why can't we have one digital system where everyone logs in and puts someone's Aadhaar card number to verify whether this person is COVID-19 positive or negative.**
>
> **UMESH MEHTA**
> EVP & Global CIO at Jubilant Life Sciences

> We need to be more proactive in managing any public emergency. We should have a robust disaster management plan, remediations, and an updated national Standard Operating Procedure (SOP) before any technology interventions. We need to connect the dots and come up with a standalone national portal so that people are not struggling to get the credible information.
>
> **PRATAP PAT JOSHI**
> CIO, Mercedes-Benz India

that the country had defeated the pandemic. In the absence of robust data collection and translation tools or disease tracking solutions at state or national levels, India failed to estimate the gravity of the situation.

One needs to remember that this is not the first time that India looked woefully unprepared for unlikely and upsetting events. In 2015, India struggled to contain the H1N1 virus and failed to develop a timely strategy to spread awareness about its prevention and accelerate vaccination drive. With COVID-19, which is considered ten times deadlier than the Swine Flu, the challenges have gone to a new level altogether.

With the country's top scientific advisors cautioning that the third wave could be even more dangerous, especially for children, the big question on everyone's mind is: Are we ready to manage the third wave of the pandemic? And what is needed to be done to ensure that such emergencies are handled well by us in the future?

According to technology experts, the country needs systematic changes in its healthcare management approach. "We need to be more proactive in managing any public emergency. As a nation, are we ready for any exigency, whether earthquake, tsunami, or pandemics? We need to move on from the mindset that if something comes in, we will address it. We should have a robust disaster management plan, remediations, and an updated national Standard Operating Procedure (SOP) before the technology can come into play," said Pratap Pat Joshi, CIO, Mercedes-Benz India.

In most countries, the national emergency warning systems have played a pivotal role in alerting the public to life-threatening disasters or crises. India's emergency response framework proved to be perilously incompetent to handle a problem of such a magnitude.

India's low digital literacy also played a crucial part in the deteriorating situation and rising number of cases. "One of the biggest reasons that made the COVID situation unmanageable in India was the inability of people and doctors' to promptly reach each other. The line of treatment for COVID-19 is almost the same with minor variations. Mostly, the cases became severe because people didn't take medicines on time," said Rajiv Sikka, CIO, Medanta Medicity.

Sikka emphasized the importance of teleconsulting through new-age platforms and the need to teach essential tech to all medical practitioners and people. "They [patients] started thinking about medicines on the seventh stage, for instance. In such a scenario, simple WhatsApp-based teleconsulting platforms could have done wonders and lessen the impact. The challenge was that both patients and doctors were facing problem in using the technology. By using basic tech, through Mohalla clinics and primary healthcare centers, doctors could have reached patients effectively by doing multiple basic consultations remotely," added Sikka.

Another big problem area during this crisis was the lack of collaboration between different entities. There was no strategic planning or coordination between government agencies, hospitals, doctors, and people. When people started facing a shortage of medicines and clinical oxygen, no one knew which way to go. It was all haphazard, with people reaching out to each other for help.

"Supply chain was not an issue. Planning was an issue. Most of the manufacturers were unprepared that something like this would happen. There was no data, no warning system. It becomes imperative for the country to collect data patterns to predict the probabilities of a virus-spread or a crisis. It is equally important to teach basic technology to the masses so that they can leverage it to their advantage," said Pooraan Jaiswal, CIO of Entero Healthcare, which is one of the largest healthcare supply chains in India.

The government should partner with top technologists to design effective surveillance systems and early outbreak warning systems to accelerate the response from health professionals and the state governments to control the outbreak's spread.

We fell ignominiously short of ideas to assess, identify, and prioritize health requirements during the response phases. Except self-declaration-based contact tracing app, Aarogya Setu, there was no primary outbreak management application or technology tool through which the country's centralized public safety management team could administrate and track the COVID-19 cases and patient's health progress. This limitation of generating accurate real-time data proved to be a significant hurdle in developing a connected healthcare ecosystem.

Automation-based technologies can also help reduce the gap between patients and doctors. By leveraging teleconsulting and video consulting facilities, especially in government hospitals, India can boost remote patient monitoring capabilities even in rural areas. Such remote management can help people take timely medical advice, enable doctors to monitor their patient's health progress remotely, particularly in areas where medical facilities are inadequate.

Data plays an essential role in managing a crisis

Despite the government ramping up its vaccination efforts, it is also true that the pandemic has long-term effects on our people's health, savings, and overall well-being. As we continue to overcome the challenges related to the pandemic and infections emerging from the second wave, digital technologies and data insights tool remains the biggest hope to maintain people's safety and well-being.

Data is exceptionally critical for delivering tech solutions that can help everyone inform about the resource availability during the response phase of the pandemic. By deploying integrated technological tools across all hospitals, clinics, and isolation centers, raw medical data of each of them can be collected in real-time to get the status of individual hospital capacity, availability of beds, and other life-saving resources through a centralized dashboard, available to all citizens to see.

"There is so much of data today which is not collected. Just like we collect data to predict customer behavior, why can't we start collecting data to identify different patterns of pandemic behavior and various conditions across the country? Can medical fraternity and corporates come together, anonymize some of the pieces of data and give it as a pool to the government so that they can form large patterns of data and derive meaningful insights?" expounded Deepak Bhosale, GM - IT, Asian Paints.

The government of Australia, for instance, demonstrated immense faith in using machine learning, artificial intelligence, predictive analytics, and natural language processing technologies to build trust in citizens and ensuring timely decisions. The country invested significant time and money to strengthen its capability to track and manage the COVID-19 outbreak.

According to a Mckinsey report titled, "Collaboration in crisis: Reflecting on Australia's COVID-19 response," in Australia, there is no shortage of information during this crisis. Both businesses and governments have had to cope with an avalanche of new and sometimes conflicting data. Australia has taken a deliberately data-led approach, harnessing the expertise and doing vital work to filter out the noise and focus on practical, trusted information to shape decision-making. A notable aspect was that each state had developed its contact tracing app very early to detect local hot spots accurately at their level and adopt tailored approaches to contain the virus. The country formed a new National Cabinet body, an inter-governmental forum to facilitate collaboration between state governments and central government.

Similarly, Taiwan, situated just 81 miles off the coast of mainland China, was one of the biggest COVID success stories that emerged during the first pandemic wave last year. The country successfully navigated the pandemic by leveraging new-age technologies, integrating its national health insurance database with its immigra-

> Data capturing, employee monitoring, and technology upgrades are happening at an organizational level, and it's time for India to connect the dots. You may talk about artificial intelligence, analytics, or any other intelligent algorithms-based platform. However, none of the technology will function unless and until a large pool of data is available.
>
> **VINOD BHAT**
> CIO, Vistara

One of the biggest reasons that made the COVID situation unmanageable in India was the inability of people and doctors to promptly reach each other. Mostly, the cases became severe because people didn't take medicines on time. In such a scenario, simple WhatsApp-based teleconsulting platforms could have done wonders and lessened the impact. Both patients and doctors were unable to use the existing technology, and that was the biggest challenge.

RAJIV SIKKA
CIO, Medanta Medicity

tion and customs database for intelligent insights and data.

The government of Taiwan developed several data intelligence templates that helped it map the virus transmission and contain it by leveraging technological solutions based on artificial intelligence and machine learning. The country was instrumental in generating real-time data based on its people's travel and medical history and separate its travel passengers after analyzing their health symptoms and recent travel data. By integrating technology in its public emergency response strategy, it was successful in containing the pandemic at an early stage.

India needs to learn from such global initiatives and build new real-time data collection frameworks to create real-time online and app-based dashboards. These centralized platforms can be instrumental in signaling the possibility of the next threat. Moreover, during the response phase of the pandemic, these platforms can accurately help generate real-time data on various critical pieces. From the availability of beds and medical resources in a nearby hospital to the shortage of necessary pharmaceutical stocks, nearby vaccination centers, and plasma requirements, these platforms can instantly update the real-time situation. Such media can enable doctors, residents, and governments to collaborate better for quality patient care.

"You can have an adaptable and responsive supply chain as long as you know what does the demand and supply look like. There are a lot of smart devices available today, and they can help analyze the trends. However, to accomplish that successfully, data has to authentic, correct, and in one place. There are a lot of cloud technologies available today which can hold even terabytes of data. On top of this integrated data layer, services, which could be micro or API-based, can be built and consumed by various government agencies or third parties for better disease prevention controls," explains Vinod Bhat, CIO, Vistara.

Need for building a digital healthcare database

Many countries have already taken robust measures to integrate technology and innovative solutions with their healthcare systems to elevate their public emergency management. The foundation for successful technology integration with a country's healthcare system depends on developing accurate healthcare databases and electronic health records of citizens.

The availability of and access to electronic health records provide doctors meaningful insights into the patient's historical medical data, such as any critical illnesses, previously taken medications, allergies, tests undertaken, among others. With big data and deep insights, this data can generate quick patterns for a doctor to help him provide a precise solution to a patient speedily and enhance hospitals' productivity during a crisis. This database can be a quick reference point for insurance agencies and other government agencies, especially during a national emergency like Coronavirus, where a physical assessment of patients may not be easily possible.

Electronic data records can help immigration teams quickly check the traveler's medical history, infectious disease history, and vaccination status even in international or national travel without any hassle. Many countries, including India, have already taken steps to launch digital health passports, integrating individual's health credentials/data.

Leading technology experts believe that India should look at the experiences of global countries and fast-track its efforts to build a digital healthcare database. "Whatever data is available today, that should be made available to the agencies. For instance, why can't the individual reports of RT-PCR, the test to detect severe acute respiratory syndrome, go into a central repository? News sources suggest that many people, with the help of photoshop, are using fake COVID-19 results for traveling purposes. There should be no need to carry that report physically. Why can't we have one digital system where everyone logs in and puts someone's Aadhaar card number to verify whether this person is COVID-19 positive or negative," said Umesh Mehta, EVP & Global CIO at Jubilant Life Sciences.

Vinod Bhat highlights the importance of capturing the data from different sources and create an integrated data layer for developing effective technology solutions. "Data capturing, employee monitoring, and technology upgrades are happening at an organizational level, and it's time for India to connect the dots. You may talk about artificial intelligence, analytics, or any other intelligent algorithms-based platform. However, none of the technology will function unless and until qualitative data is available," Bhatt adds.

To build a robust national defense against public healthcare emergencies, India needs speedy efforts to develop a digital healthcare database of its citizens. And boost its capabilities to generate centralized raw data from hospitals and pharmacies to help it develop cutting-edge AI-based public emergency surveillance tools and effective data insights platforms. One such area is wellness management, which focuses not only on a particular disease or virus but also on a person's overall well-being. It is not just the pandemic and infection, but also many other aspects that people struggle with during the post-COVID phase. The pandemic has affected almost everyone in some or another way. The scars are deep!

Many people have lost their loved ones. Many are dealing with post-disease complications, isolation and several others are facing the deterioration of mental health and continuous distress. Technology can play a pivotal role in ensuring good physical and mental health for all residents. Identifying people in need and providing them regular counseling should be on priority for the government. A centralized wellness app, an enhanced version of Aarogya Setu, can also be introduced by the government, enabling citizens to refer to the handy resources related to a public emergency and seek immediate counseling.

Key Tech Solutions for COVID Management

- **Early outbreak warning systems:** Early outbreak warning systems are intelligent surveillance systems that gather data from various sources to forecast future disasters and generate an immediate response to control the situation.
- **Improved medical diagnosis:** Through advanced ML/AL techniques, innumerable imagery data of patients can be filtered, segregated, and analyzed, providing detailed results of the patient's health condition and recommend better diagnosis/treatment.
- **Deep learning based pandemic forecasting models:** A subset of AI, deep learning uses many layers to investigate historical data such as the number of hospitalizations, cases, and deaths, and analyze current data to create a hypothetical impact of the pandemic and forecast its transmission rate. By analyzing individual patient's electronic health records, the AI-based tools can help doctors deliver customized and timely treatment for each patient.
- **Real-time dashboards/Digital Command Centers:** During the response phase of the pandemic, raw data around COVID can be generated through contact tracing apps, social media, hospitals, test laboratories, and other data-driven tools to update the status of availability of beds, ICUs, medical essentials, vaccinations, and plasma requirements in various hospitals. With AI, such data can be further analyzed to check the status of shortage of medical essentials at different hospitals or localities. Such platforms can enable doctors, residents, and governments to transform the medical services and patient experiences.
- **Virtual patient wards:** Modern digital devices, mobile sensors, and video teleconsulting enable physicians to monitor patient's health remotely. Doctors can manage mild to moderate symptoms cases through online patient wards. Infected patients can input their day-to-day symptoms, recovery development, or deteriorating condition and accordingly get the appropriate counseling from the doctors and immediate interference of the medical team if needed.
- **Conversational chatbots:** AI-based chatbots can prove to be an effective tool to support COVID patients by providing them accurate information about the disease, pre- and post-COVID care. Their conversational interface, if designed well, can answer multiple questions, and also help residents find vaccination availability and slots in hospitals near to them.
- **Medical oxygen and essential drugs/medicines trackers:** Forecasting the demand, stock availability, medical-grade oxygen availability, and crucial medical supplies can be tracked and managed through central ERP-based software. Moreover, by installing the Vehicle Location Tracking (VLT) devices, all tankers/medical vans used for medical essentials and oxygen transport, proper monitoring of their location, safety, and timely supply can be ensured by hospitals and the government.

Supply chain was not an issue. Planning was an issue. Most of the manufacturers were unprepared that something like this would happen. There was no data, no warning system. It becomes essential for the country to collect data patterns to predict the probabilities of a virus-spread or a crisis. It is equally important to teach basic technology to masses so that they can leverage it to their advantage.

POORAAN JAISWAL
CIO, Entero Healthcare

"Wellness management is coming up as a big subject. Even if you are visiting different physicians or hospitals over a while for treatment, your data should be available to them to track and suggest requisite measures. The government should leverage technologies such as artificial intelligence to give early warnings and recommendations to people based on their health conditions. Of course, this entire process of automating records needs to be implemented, keeping data privacy issues in mind," said Rajesh Uppal, Executive Officer (EO) - IT and CIO of Maruti Suzuki India.

Impactful and timely communication

In a country as diverse as India, communicating in a national emergency becomes paramount to fight pandemics and safeguard healthcare. Since the beginning of the pandemic, there has been a flood of information, and not all are authentic.

For example, at the peak of COVID-19, the country saw massive discrimination against healthcare workers and their family members. Many healthcare professionals received hostile behaviors by their communities and residential societies due to the faulty reasoning and the misconception that they are more vulnerable to contagious disease and can be COVID super-spreaders.

The Indian government's failure to establish trusted pandemic broadcast channels across all platforms also played a massive role in the community transmission of the virus. It resulted in people relying on many peculiar theories about the pandemic and homemade cures, putting people's lives at risk.

The condition of the villages is even more dismal, where there is a significant dependency on hearsay to combat any such situation, and misinformation spreads like fire. The government needs to develop a strategy to deliver impactful communication around disease prevention by engaging local talent in villages and far-flung areas, identifying few residents, and getting them trained in basic technology platforms and dashboard data access and analysis.

These residents can be a one-single point of contact for a central risk management team, taking regular updates and providing necessary guidance, and circumvent any misleading or false information about any aspect of the disease.

In addition, the government should strengthen its disease surveillance system and enhance its ability to broadcast important messages through SMSes, mobile apps, social media videos/apps, mobile calls, radio, and television. Automation of delivering such messages can play a crucial role as well. We need to focus on building innovative messaging mechanisms to increase the frequency of such broadcasts for positive COVID patients.

AI-based chatbots can prove to be an effective tool to support COVID patients by providing them accurate information about the disease, pre- and post-COVID care. Their conversational interface, if designed well, can answer multiple questions, and also help residents find vaccination availability and slots in hospitals near to them.

These interactive chatbots can increase the recovery chances of COVID-19 patients at home and ensure the timely implementation of precautionary steps to prevent the spread of the disease. Such technology-driven initiatives can help reduce the burden on hospitals overwhelmed by patients infected with COVID-19 while raising public awareness about the perils of misinformation.

The way ahead

The current crisis should be the final wake-up call for India to set aside a larger pool of investments to integrate the country's healthcare with the latest technological advancements! Besides developing robust data pools, it is also critical for the government to review the national and state-level crisis response plans and the capabilities required to manage pandemics.

"Similar to the organizational approach, there has to be a strong contingency planning in detail by classifying disasters at national and state levels. The entire concept of business continuity planning needs to be extended to the government as well. It is getting done but so far at a limited level. The time has come for a complete reassessment about our existing state, and we need to learn how advanced countries have gone ahead in managing public emergencies, a lot of which looks proactive and well-prepared. The last two waves have given us enough data and experiences to lay down something which should probably scale up in the future," explicated Deepak Bhosale.

In addition, there is a strong need to make backup funding available to deploy digital technologies and data-driven tools across hospitals, pharmacies, and crisis monitoring agencies to keep track of medical stocks, bed requirements, and patient health status. "Whatever is available, we need to start from there and thinking about connecting the dots to cover the entire value chain. Let's ensure that the relevant people have visibility around the information and data that helps them address the basic problems people face during a health emergency," recommended Umesh Mehta.

Rapid efforts are required to digitize medical records, develop AI-based warning detectors, set up a robust telemedicine program, and automate time-consuming processes such as patient check-in at a hospital for better patient care. People should be encouraged to take phone and video consultations with doctors, and this facility should be made available across government hospitals in India. At the village and district level, there should be a high focus on talent transformation and creating a pool of people who understand the technology, access relevant information, and address basic medical queries of the public.

To boost teleconsulting and video consulting, the Indian Medical Association needs to relook at its rulebook, preventing patients from consulting doctors licensed in a different state. It will reduce India's overwhelming healthcare system burden during a public emergency. Government and corporates should step in to develop digital command centers, which are online information hubs where all resources and credible information around a public crisis can be kept for quick reference.

By broadening the canvas of data capturing, collecting them in one place, and linking the fragmented dots in the current system, the government can effectively address the existing fault lines and gaps in managing public emergencies. On top of this data layer, different solutions and services can be built and help India move from reactive to proactive to productive healthcare management. ■

Wellness management is coming up as a big subject. Even if you are visiting different physicians or hospitals over a while for treatment, your data should be available to them to track and suggest requisite measures. Administrators can leverage technologies such as artificial intelligence and machine learning to give early warnings and recommendations to people based on their health conditions. Of course, this entire process of automating records needs to adopt keeping data privacy issues in mind.

RAJESH UPPAL
Executive Officer (EO) - IT and CIO of Maruti Suzuki India

There is so much of data today which has not been collected. Just like we collect data to predict customer behavior, why can't we start collecting data to identify different patterns of pandemic behavior and various conditions across the country? Can we all come together – medical fraternity, corporates – anonymize some of the pieces of data and give it as a pool to the government so that they can form large patterns of data and derive meaningful insights?

DEEPAK BHOSALE
GM - IT, Asian Paints

FinTech Start-Ups Are Going To Be The Next Big Employment Creators

India has become Asia's largest destination for FinTech investments, overtaking China and is on the cusp of a FinTech revolution

By Robin Bhowmik

To say that the FinTech sector in India is among the fastest growing industries of the country would be a gross understatement. India has become Asia's largest destination for FinTech investments, overtaking China and is on the cusp of a FinTech revolution. In fact, a large chunk of India's unicorn start-ups over the last few years have been FinTech companies. It is estimated that India's FinTech market will reach USD 150 billion by 2025.

The various FinTech domains are InsurTech, digital lending systems, digital payment gateways, microfinancing solutions etc. FinTech products are designed to streamline financial service delivery by being virtual, paperless, customizable and oriented towards addressing a highly specialized need instead of a one-size-fits-all alternative, e.g., cab-ride insurance, micro-loans for specific purchases and apps like PhonePe, Google Pay and the like.

The factors responsible for the rapid growth of FinTech in India are two-fold. Firstly, the COVID pandemic has seen digital payments rise significantly in India, not only in metros, but also in tier 3 and tier 4 cities. Amidst COVID, India saw a 60% increase in FinTech investments. Secondly, as FinTech products are highly customizable and cheap and do not require high service fees, long approval times and unnecessary documentation. FinTech has made financial services accessible to millions of customers from the low/middle income group, which largely constitute the Indian middle class. A great example of such a product is Paytm's INR 2 lakh within 2 minutes loan or Bajaj's gym injury insurance.

As digital adoption continues to grow over the next few years, the FinTech sector will likely remain a lucrative investment market, leading to the entry of new players and innovative products.

The entry of more players into the FinTech space will also open up tremendous job opportunities for software engineers, provided they equip themselves with the right tools and channel and market their skills effectively. As a result, in the near future, there is likely going to be a huge demand for a skilled workforce in the FinTech sector in the following areas.

Cybersecurity

The COVID-19 pandemic has created huge opportunities for financial technology companies. Financial institutions are adopting fintech solutions to mitigate the risks posed by the threats that the digitisation has brought. However, along with this speedy tech transformation, new cybersecurity risks are also emerging. This makes it imperative for fintech startups to take appropriate measures to secure their ecosystems from being compromised.

There is a huge skill shortage in Cybersecurity in India. According to a report by website, Comparitech, India ranks 15th worst in the world among the 60 countries surveyed in cybersecurity. According to a survey conducted by ISACA (Information Systems Audit and Control Association), which is an international professional association focused on IT governance, 87 % companies responded that there is a shortage of skilled cybersecurity professionals in India and only 41 % respondents felt they are ready to guard themselves against a cyber-attack. As fintech companies rely enormously on usage of applications which involve end users to fill in sensitive data and transferring of money with a one touch, to build these robust applications need of professionals with impeccable skill sets is required.

Blockchain

India has witnessed significant rise in the jobs catering to blockchain and cryptocurrencies, and pandemic has added to the demand of such profes-

As digital adoption continues to grow over the next few years, the FinTech sector will likely remain a lucrative investment market, leading to the entry of new players

sionals hugely. Gartner predicts the business value of Blockchain tech will exceed USD 3 million by 2030 and the skill set of blockchain professionals will be one of the fastest-growing skill sets – growing at a rate of 2,000 – 6,000%. The demand for Blockchain developers is not only limited to the BFSI Sector anymore. It is also witnessed in Healthcare, Education, Supply chain management, cloud computing, stock trading, real estate and even government agencies. Owing to the talent gap in this domain, it has been observed that employers are ready to pay high remuneration to professionals who have solid technical background and are ever curious to learn about new technologies. It has been observed that the salary of a Blockchain techie is higher than an average IT professional and with the right skill sets a Blockchain professional can also make twice the salary of what a Software Engineer may make in a year.

The FinTech boom is here to stay for the foreseeable future and there is much to be optimistic about employment opportunities in the sector. Expect a lot more companies to enter

Full Stack Developer

The role of Full Stack Developers is one of the most talked about professions in the year 2021. A Full Stack Developer is some with knowledge in front-end layers like HTML, CSS, JavaScript, Logic layers with programming languages like Python, Java, PHP, and Data Layers like SQL, Oracle, etc. For FinTech companies, it is much more beneficial to hire Full Stack developers instead of hiring separately for front-end and back-end like easier and faster troubleshooting, time and money savings being some of the more obvious advantages. The demand for this profession is skyrocketing due to tremendous adoption of digital transformation in the country. All industries, from startups to multinational corporations in businesses, are scouting for full-stack developers. As different projects require different skills, no two full-stack developers have the same skills. They are of value, demonstrating to be highly versatile assets to the organization. Their hold in knowledge, field-expertise, and adept technological insight has proven to be highly valuable to organizations. With the enormous profits that accompany hiring a full-stack developer, companies, mostly startups which have a financial clockwork that is ticking continuously, aim to employ them in comparison to individual stack developers.

Data Analysis

Demand for people with specialized data skills sets is multiplying every year. More and more fintech startups and organizations are understanding the importance of capturing, interpreting, and being informed by data. Such data-driven insights can not only radically transform businesses but also help target new markets, address customer pain points, boost revenue and much more. Even organizations in the research and administration sector can amplify the success of their daily activities by leveraging data science practices and tools. So, it is no brainer that the job market demand for data science professionals like data scientist, data architect, data analyst is growing every day. As the FinTech industry is heavily reliant on data. But just accumulating data isn't enough. They need experts to mine and interpret it. Data Analysts provide concrete solutions and recommendations on how products and services can be improved. With growing usage in IoT, Data Analysts will be in huge need in fields like healthcare, manufacturing sector, and other private and public industries, making it one of the most sought-after jobs. Research by Analytics Insight predicts there will be 3 million job openings in Data Analytics by 2021-22.

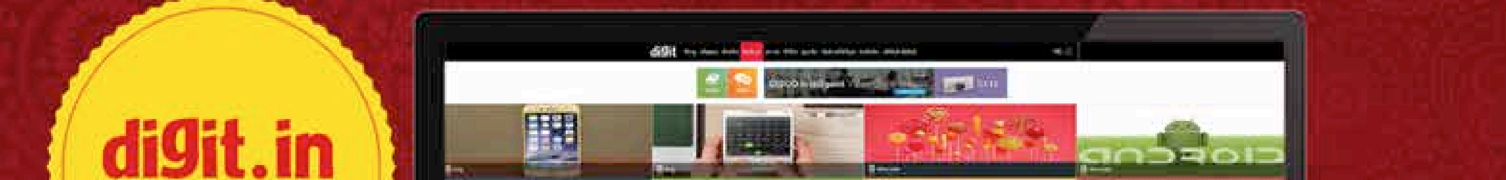
The FinTech boom is here to stay for the foreseeable future and there is much to be optimistic about employment opportunities in the sector. Expect a lot more companies to enter this space in the upcoming years. Companies that will be scouting for employees to build and maintain a robust and scalable FinTech infrastructure. For software engineers, this means opportunities galore. With the right skills and direction, the FinTech job market is theirs for the taking. ■

The author is Chief Business Officer of Manipal Global Academy of BFSI

डिजिट

अब हिंदी में

देश का सबसे लोकप्रिय और विश्वसनीय टेक्नोलॉजी वेबसाइट डिजिट अब हिंदी में उपलब्ध हैं। नयी हिंदी वेबसाइट आपको टेक्नोलॉजी से जुड़े हर छोटी बड़ी घटनाओ से अवगत रखेगी। साथ में नए हिंदी वेबसाइट पर आपको डिजिट टेस्ट लैब से विस्तृत गैजेट रिव्यु से लेकर टेक सुझाव मिलेंगे। डिजिट जल्द ही और भी अन्य भारतीय भाषाओ में उपलब्ध होगा।



www.digit.in/hi
www.facebook.com/digithindi

डिजिट

The Rise And Rise Of Big Breaches

That is the bad news. The worse news is....they may just be the more visible type of incidents

By Shyamanuja Das

On 25 April, security watcher Alon Gal (@UnderTheBreach) tweeted that infamous threat actor, 'ShinyHunters', had just then leaked the database of Indian online grocery store, BigBasket. Gal, Co-Founder & CTO of cybercrime intelligence firm, Hudson Rock, also posted the screenshots, in his tweet. He said information, such as emails, names, hashed passwords, birthdates and phone numbers were leaked.

The news of the breach per se was not new. The actual breach happened in October last year and made it to the headlines for its size—20 million users' data got stolen—and the way BigBasket reacted to it.

For the uninitiated, here are the timelines of the breach, provided cyber intelligence firm, Cyble, in its blog. Cyble had first detected this breach. According to the firm, the breach happened on 14 October 2020. It was detected by Cyble on 30 October 2020. After verifying, the firm reported this to BigBasket on 1 November 2020.

"Cyble disclosed the breach to BigBasket management per the responsible disclosure process. Praveen (BigBasket) strongly insisted for not making any disclosure. Cyble advised them to let their customers know and explained to them it's the right thing to do," the blog said.

BigBasket was not the only company affected. Cyble began notifying their customers about the breach. The firm claims it was approached by BigBasket help them on the breach, on which Cyble insisted on the disclosure to BigBasket customers first.

According to a report in OpIndia, Cyble was actually named in the FIR registered by BigBasket on 6 November, with the cyber cell of Bengaluru Police.

On 7th November, Cyble made a public disclosure. And two days after that, on 9th November, BigBasket acknowledged the breach, as reported by Bloomberg News.

After Cyble made it public and BigBasket acknowledged the breach, it made it to the headlines in most business media. It raised a lot of interest in general media, thanks to familiarity of the brand among common users of online purchase, which has risen significantly post the pandemic hit India in March that year.

It is almost after six months that the issue has taken center stage again. The hackers have put up the data after so long. A report by News18 confirmed that the post contains a 3.25GB database that includes "a varying degree of personal information belonging to over 2 crore individuals." The report said the database file has phone numbers, residential addresses, dates of birth and email addresses, among others.

The BigBasket case shows that even now, there is a reluctance to disclose data breach in India. The reason why it came out was because the cyber intelligence firm was vocal about it. And also, the brand being well-known, general media got quite interested in the breach.

But by no means is BigBasket breach the only example of its kind. Post pandemic, in India alone, there have been number of such data breaches.

The more recent ones (March-April 20221) have been in Domino's India (Jubilant Foodworks) where data of 180 million orders were stolen. According to Gal, credit card details of 1 million customers were also compromised, though the company has denied it. In another similar breach, online trading company, Upstox, said its user data got breached. Though Upstox did not put a number to it, most media reports have put the figure of compromised users record as 2.5 million. Another alleged data breach happed with mobile payment company, MobiKwik, where security watchers put the figure of compromised records as 3.5 million.

Even now, there is a reluctance to disclose data breach in India

There is a pattern to all of this.

All of these have happened with online businesses. While three of them are pure online businesses, the fourth one - Domino's - has also shifted significantly to online ordering from phone-based ordering, especially during the pandemic.

BREACHSCAPE

COMPANY	MONTH	ALLEGED* DATA COMRPOMISED/EXPOSED
Domino's India (Jubilant Foodworks)	04/21	180 million orders, 1 million credit cards
Upstox	04/21	2.5 million users data
MobiKwik	04/21	3.6 million KYC data and 99 million other sensitive data
Police exam database	02/21	0.5 million (10,452 samples shared online)
Airtel J&K (alleged)	02/21	2.6 million users data
Juspay	01/21	100 million (alleged), 35 million (acknoweledged, masked data)
WhiteHatJr	11/20	0.28 million students data
Haldiram's	10/20	NA
PM's personal website	10/20	0.57 million donors data
Bharat Matrimony	10/20	NA
IRCTC	10/20	0.9 million users data
Dr Reddy's	10/20	NA
Edureka	09/20	2 million users data
Paytm Mall	08/20	NA
Dunzo	07/20	3.4 million users data
Unacademy	05/20	20 million users data
BHIM payment system	04/20	7 million users data

**The information is compiled from media reports and company announcements. In many cases, the companies have either denied or not made the number public, while acknowledging there was a breach.*

The new drivers of security issues can be summarized as two Ds—Digitization and Distributed workforce. While digitization expanded the threat surface, distributed workforce working remotely created conducive environment for targeted attacks

The New Normal?

Between April 2020 and now—the period since the pandemic started impacting businesses leading to faster digitization—there have been dozens of data breach incidents.

Are data breaches the New Normal?

Well, the answer to that depends on how you interpret the question. If you go by the literal meaning, of course, all these examples (see Breachscape) point to that.

But data breaches could also be just the more visible type of incidents. Unlike many other incidents, data breaches are easier to track by external agencies. Despite all evidences pointing to the breaches, many companies outrightly reject, target the agencies reporting these breaches by following a shoot-the-messenger approach.

It can well be imagined how many other incidents could be reported and discussed. So, while data breaches—at least to some extent—are public and discussed, other incidents are not. Reports suggest there have been rise in all kind of security incidents.

And there are reasons for that. The new drivers of security issues can be summarized as two Ds—Digitization and Distributed workforce. While digitization expanded the threat surface, distributed workforce working remotely created conducive environment for targeted attacks.

An ISACA survey released earlier this year said 87% organizations believe rapid shift to work from home increased risk of data privacy and protection issues.

All the data breaches, given in the table, Breachscape, for example, happened post-April 2020. Other kind of incidents too have increased significantly, so much so that businesses have been forced to look at cybersecurity as a basic business enabler.

Nearly 96% respondents in a recent research by PwC, Global Digital Trust Insights Survey 2021, said that they will adjust their cybersecurity strategy due to COVID-19. As many as 50% are more likely now to consider cybersecurity in every business decision — up from 25% in the same survey last year.

There are numerous research reports that confirm this realization that organizations need to be far more proactive about cybersecurity post-pandemic. ■

The Changing Contours Of Global Technological Risk

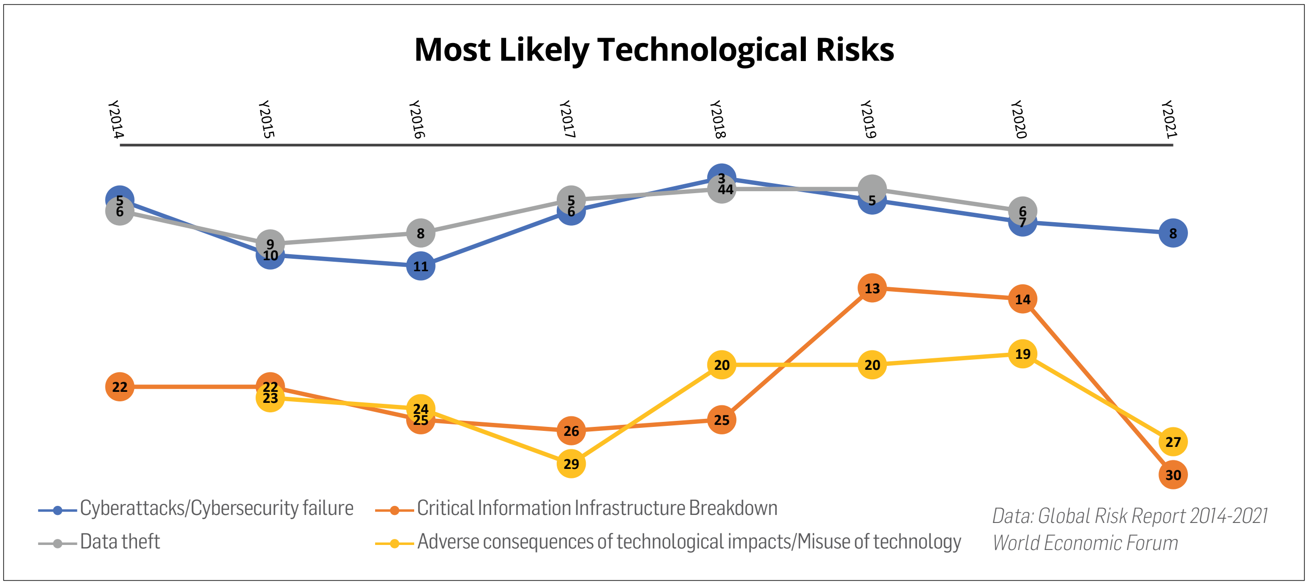
Why we need to look beyond just cybersecurity...

By Shyamanuja Das

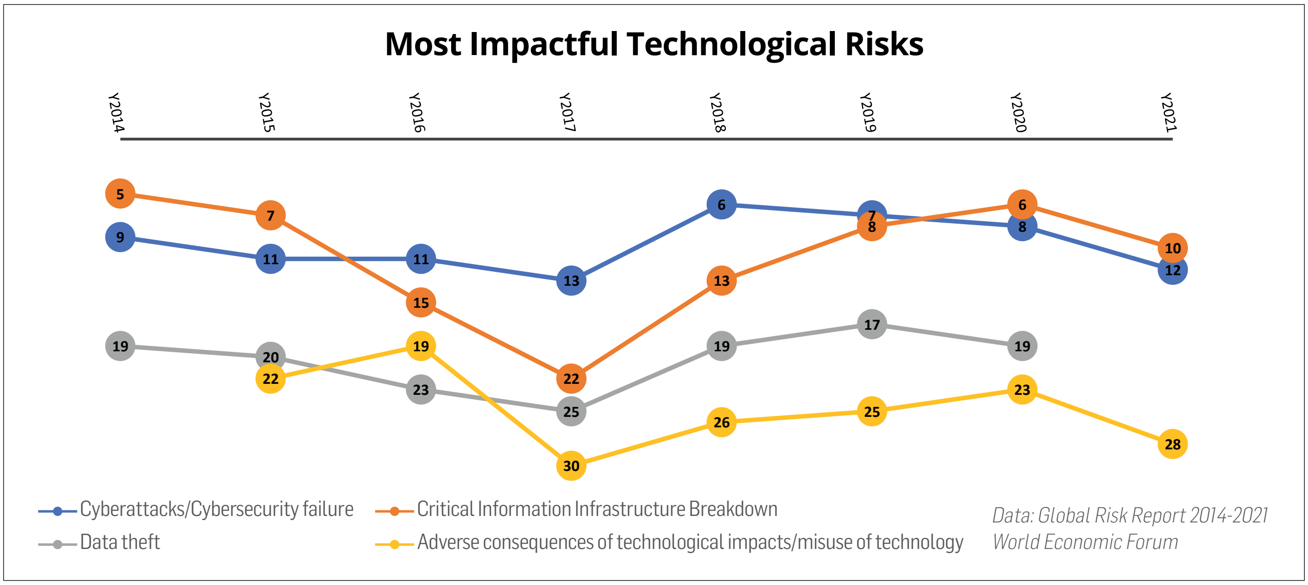
The annual Global Risk Report of the World Economic Forum (WEF) is a good barometer to gauge what constitutes global risk at any point of time. Released just before WEF's annual meet in Davos, the major highlights of the report make it to news headlines during that time.

That reflects the tone and nature of the report, as it deals extensively with the risks for that year, with some comparison with the previous year. Since it is targeted at global business decision makers and policymakers, it serves that purpose very well. The report's stated objective is to sensitize 'about the need for a multi-stakeholder approach to the mitigation of global risk.' However, considering the periodicity of the study and a longitudinal nature of the study, it can also be analyzed to understand how the risks have changed over the years.

This article attempts to do just that, albeit in one of the risk areas that is of interest to our readers. The GRR has been classifying all risks into four buckets or types of risks—economic, geopolitical, environmental, and technological. This year's report, for example, has considered seven economic risks, six environmental risks, seven geopolitical risks, nine societal risks, and six technological risks, totalling 35 global risks. Not surprisingly, Infectious diseases, as a risk, has jumped from 9th position in 2020 to the top position, among the most impactful global risks in 2021. It is how the likelihood and perceived impact of technological risks have changed over the years that we are going to discuss here. Till 2020, the GRR considered four technological risks – Cyberattacks, Critical information infrastructure breakdown, Data fraud or theft and Adverse conse-



Data: Global Risk Report 2014-2021
World Economic Forum



Data: Global Risk Report 2014-2021
World Economic Forum

quences of technological impacts/ Misuse of technology.

This year, it has dropped data fraud or theft from the list of technological risks and has added three new risks – Digital inequality, Digital power concentration and Failure of technology governance. One more risk – Cyberattacks – has been replaced by Failure of cybersecurity measures, thus acknowledging the overall awareness about cyberattacks and measures to curb them. The risk, hence, now is failure of those measures!

From the time IT NEXT has been tracking the GRR—that is from 2014 onwards —Cyberattacks and Data fraud or theft have always been considered among more likely risks, with Data fraud or theft featuring among the top 10 since 2014. Cyberattacks too have featured among the top 10 most likely risks in GRR in all years except one. Both Critical information infrastructure breakdown and Adverse consequences of technological impacts have always been perceived as comparatively low-probability risks.

When it comes to impact of technological risks, data fraud or theft, the most common risk, has never been seen as a very high-impact risk. Cyberattacks, on the other hand, have been seen by GRR respondents as a more impactful risk, featuring between 6th to 13th position in various years. Critical infrastructure breakdown has moved with technology disruptions. In the early phase of cloud, 2014-2015, it was seen as a high-impact risk. As technology matured, the risk perception came down, even going to 22nd position in 2017. Massive disruptions in services at SouthWest Airlines and Delta Airlines in 2016, in British Airways in 2017 and subsequently outages in SouthWest Airlines, American Airlines, JetBlue, Delta Airlines, Air India, British Airways, National Stock Exchange, and Hong Kong Exchange in the next two years, all of which

The six global technological risks, as defined by the GRR

Adverse outcomes of technological advances

Intended or unintended negative consequences of technological advances on individuals, businesses, ecosystems and/or economies: AI, brain-computer interfaces, biotechnology, geo-engineering, quantum computing, etc.

Digital power concentration

Concentration of critical digital assets, capabilities and/or knowledge by a reduced number of individuals, businesses or states, resulting in discretionary pricing mechanisms, lack of impartial oversight, unequal private and/or public access, etc.

Breakdown of critical information infrastructure

Deterioration, saturation or shutdown of critical physical and digital infrastructure or services as a result of a systemic dependency on cyber networks and/or technology: AI-intensive systems, internet, hand-held devices, public utilities, satellites, etc.

Failure of cybersecurity measures

Business, government and household cybersecurity infrastructure and/or measures are outstripped or rendered obsolete by increasingly sophisticated and frequent cybercrimes, resulting in economic disruption, financial loss, geopolitical tensions and/ or social instability.

Digital inequality

Fractured and/or unequal access to critical digital networks and technology, between and within countries, as a result of unequal investment capabilities, lack of necessary skills in the workforce, insufficient purchase power, government restrictions and/or cultural differences.

Failure of technology governance

Lack of globally accepted frameworks, institutions or regulations for the use of critical digital networks and technology, as a result of different states or groups of states adopting incompatible digital infrastructure, protocols and/or standards.

happened because of infrastructure issues—and not because of targeted attacks—made people realize the massive impact they could have on business and life around the world. The IT infrastructure was no more as invincible as it was thought to be. Expectedly, the risk perception in terms of impact of Critical information infrastructure breakdown, again rose, from as low as 22nd in 2017 to 6th in 2020, before dropping a few places this year. Not surprisingly, critical infrastructure breakdown is listed by GRR 2021 as the 10th most impactful global risks. It is also the most impactful technological risk, among all the technological risks considered by the GRR study this year.

The New Risks

As mentioned above, GRR has considered three new technological risks: Digital inequality, Digital power concentration and Failure of technology governance.

Digital inequality, according to the World Economic Forum, is unequal access to critical digital networks and technology, between and within countries, because of a variety of reasons. While on the face of it, it seems like a country-level risk, businesses in developing countries will be exposed to this risk—both because of unavailability of technology, inability to invest and lack of access to skilled manpower. But a more serious implication for India is lack of access to digital technology, despite cheaper phones and low cost of data. Language, availability of network access and regulatory restrictions are still pressing issues that are preventing many businesses to exploit the opportunity that lies across the country. We were badly exposed to this inequality, especially in education during the pandemic. This is a risk that no company, especially a consumer business, can ignore anymore.

Digital power concentration, on the other hand, is concentration of critical digital assets, with a small set of companies, individuals and countries. The manifestation of this could be driven by regulation, historical evolution of technology, IPR or even international trade restrictions. The pandemic has exposed us to the risk too.

Finally, failure of technology governance is WEF's term for lack of globally accepted frameworks and standards. While WEF is concerned about 'globally accepted', in the local level too, this can create a huge risk. Today, a lot is being talked about AI, which works on data. Take healthcare. To make some meaningful decision on diagnosis of patients using AI, different healthcare providers should have compatibility in their data. Without well-defined standards, this will become a Herculean task and the possibility of any significant success is remote.

The need for revaluating risk analysis

As is evident from the GRR, certain newer risks need to be taken cognizance of for any effective risk mitigation plan. Some of them have more significance for India. For example, digital power concentration is a risk that should be addressed before it becomes a monster!

As such, the pandemic has led to wider digitization as well as distributed working. The traditional cybersecurity risks are going to be very different in the New Normal. Because of more digitization, the risk surface has increased. Remote working has given rise to newer types of attacks. So, many companies are anyway looking at risk management with a fresh approach. It is imperative that they look beyond the traditional cybersecurity risks and take into account, the emerging new risks. ■

Tata Steel Leverages Blockchain For Trade Finance With HSBC

The live trade finance transaction involved the export of steel by Tata Steel, India to Universal Tube & Plastic Industries, UAE

By ITNEXT

Tata Steel has successfully executed a blockchain enabled, paperless trade transaction - a global first for the steel industry.
The live trade finance transaction involved the export of steel by Tata Steel, India to Universal Tube & Plastic Industries, UAE.

This successful execution was done by Tata Steel, in collaboration with HSBC. The end-to-end paperless trade transaction, executed over the Contour platform was made possible by a collaboration pivoted by Tata Steel across the spectrum over the Contour and essDOCS platforms. The Letter of Credit (LC) was issued by HSBC UAE for Universal Tube & Plastic Industries, UAE (importer) with HSBC India as the advising and negotiating bank for Tata Steel, India (exporter).

This transaction validates the commercial and operational viability of blockchain as an alternative to conventional exchanges for paper-based documentation. Tata Steel has also signalled its intent to explore similar opportunities in other geographies in future.

"Adoption of this platform is in line with our objective of agility and enabling a faceless yet trustworthy all-time interface to better customer experience. This unique initiative, executed in collaboration with HSBC, demonstrates our continued efforts to lead technology led disruptions by challenging the status quo and reimagining the global trade set-up," said Peeyush Gupta, VP, Steel Marketing & Sales, Tata Steel.

"This transaction is a significant step towards the mass commercialization and adoption of this technology and we look forward to its transformative impact on trade finance," added Hitendra Dave, Head - Global Banking & Markets, HSBC India.

How it works

Contour, which has been built on blockchain technology has enabled comprehensive digitization of the end-to-end Letter of Credit transaction including the e-presentation of trade documents. Contour enables the underlying LC trade transaction to be fully digitized from the LC issuance to the presentation of documents. It also enables transaction parties to transfer, manage and present electronic Bills of Lading (eB/Ls) and supporting documents within its platform via the interface with essDOCS' CargoDocs platform.

Benefits

With trade documents digitized, corporates can reduce the costs associated with handling paper-based documents, its reconciliation and streamline their processing flow. The use of blockchain technology in trade finance enables comprehensive visibility for all involved parties and enhanced security. Importantly, it helps to significantly reduce the document negotiation and banking transaction cycle times from week(s) to a few days, thereby aiding unlocking of working capital for businesses. It also helps to increase the velocity of trade, particularly in situations where shipping routes are relatively short.

This transaction validates the commercial and operational viability of blockchain as an alternative to conventional exchanges for paper-based documentation. Tata Steel has also signalled its intent to explore similar opportunities

While blockchain has been deployed for trade financing in other industries, it is a first for the steel industry in India.

Globally, steel industry is waking up to the possibility of blockchain. Apart from document authentication, which is the primary use case for the Tata Steel, the industry, known for its complex supply chain, is looking for leveraging smart contracts and tracking goods end to end on the supply chain. China's state-owned steel maker, Baosteel, launched a blockchain-based supply chain financed solution in 2018. This helps smaller suppliers to raise finance.

China's National Association of Metal Material Trade, the country's primary trade association for metals, is working on a blockchain consortium to cover the entire steel supply chain in the country.

Blockchain has been used extensively in trade finance, especially in helping smaller suppliers finance their working capital through invoice discounting ■

New Devices Introduce New Holes In The Security Framework

By converging networking and security, CISOs can ensure that dynamic changes to the network are automatically protected without impacting performance or productivity, ensuring the best user experience for employees and customers alike

By Rajesh Maurya

The demand for Digital Innovation (DI), driven by shifting markets, evolving consumer expectations, and digital competition, has done far more than just transform networks. It has completely changed the organization, including how lines of business are structured, how teams and individuals collaborate, where and how employees work, how success is measured, and how leaders execute against business objectives.

One of the most profound changes has been the increased reliance on applications to support every aspect of the business. This has led to a number of critical structural changes, such as the adoption of cloud-based infrastructures, the adoption of SaaS applications and services, and the need to provide fast, flexible and secure connections to these resources to any user on any device in any location. The COVID pandemic accelerated the adoption of innovative work-from-home solutions to accommodate the need for social distancing while maintaining business operations. Others, such as implementing network upgrades or expanding network edges, are designed to improve a company's efficiency and customer experience.

However, this need to compete in today's digital world also means that many of these business-critical initiatives can only be realized by deploying new systems and solutions. But deploying new devices as part of a DI initiative also increases the complexity of network environments and creates new security and operational complexities that open up an organization to new cyber risks.

Part of the problem occurs when a security team attempts to address new risks, especially in a new edge environment, by deploying point security products inside the growing digital attack surface. However, the additional complexity associated with monitoring and managing these point solutions, exacerbated by new data protection regulations, actually fragments visibility and reduces control, leaving security teams less prepared to protect the organization against new cyber threats, especially those that utilize a multi-vector approach.

...the cybercrime industry continues to grow. Overburdened security teams, stretched thin across the expanding attack surface and suffering from the cybersecurity skills gap, are often unable to keep up

New Devices Create New Threats

When DI initiatives add new devices and work locations to the distributed network, they not only expand the organization's attack surface but they can also introduce new holes in the security framework. These new systems and solutions typically include Internet-of-Things (IoT) devices, mobile devices, distributed cloud computing, new branch locations, and home offices.

Each one of these introduces new threats that have to be monitored and responded to by security teams. IoT devices often use insecure protocols that can't be patched and default passwords that are targeted by malware. Mobile devices commonly hop between being on- and off-network, potentially dragging malware with them behind the corporate firewall. And home offices often include older, unpatched devices that can be easily exploited and used as conduits back into the corporate network. When these solutions are protected with different, isolated point security products, it can be impossible to deploy, manage, and ensure consistent policy enforcement or to correlate threat events across the network.

Cloud computing, for many organizations, is especially challenging, as nearly three-quarters of cybersecurity professionals have trouble understanding the foundational cloud shared responsibility model. Next-gen branch networks expand security requirements as each new location has devices that must be secured. And for organizations increasingly relying upon latency-sensitive Software-as-a-Service (SaaS) applications, relying on traditional connections to apply corporate security solutions also means routing all traffic through the headquarters network, impacting user experience, and the bandwidth required to scan these applications for malware simply exacerbates the problem.

Similarly, telework introduces new challenges, such as relying solely on VPN connections to provide security. VPNs do not inspect traffic. A compromised home network simply means that a VPN provides a secure tunnel through which bad actors can inject malware into the corporate network. Monitoring and securing these new devices and environments often requires specialized security tools, increasing the workload overhead on security teams.

Growing Cyber Threats Versus the Cybersecurity Skills Gap

At the same time that networks are being transformed, the cybercrime industry continues to grow. Overburdened security teams, stretched thin across the expanding attack surface and suffering from the cybersecurity skills gap, are often unable to keep up. Deploying "best-of-breed" standalone cybersecurity solutions to address

Rather than enhancing security, this level of vendor and solution sprawl actually diminishes their ability to not only detect, but also defend against active attacks

each potential attack vector as it is discovered simply makes the problem worse. Recent research shows that IT teams now have an average of 45 security solutions deployed across their networks. Rather than enhancing security, this level of vendor and solution sprawl actually diminishes their ability to not only detect, but also defend against active attacks.

Complicating this problem further is the lack of integration between these tools. This means security teams must manually collect, aggregate, and analyze data from multiple platforms to gain the context required to detect and remediate threats on their networks. Leveraging expert security analysts might save time by collecting only a subset of significant data. But such experts are hard to find with a cybersecurity skills gap of over 3 million unfilled positions has left organizations understaffed and existing teams overworked. The addition of new devices and solutions that require manual security processes absorb essential time from security teams. And this is made worse because these manual correlation processes do not scale with the frequency and complexity of cyberattacks.

Solutions for Securing Digital Innovation Initiatives

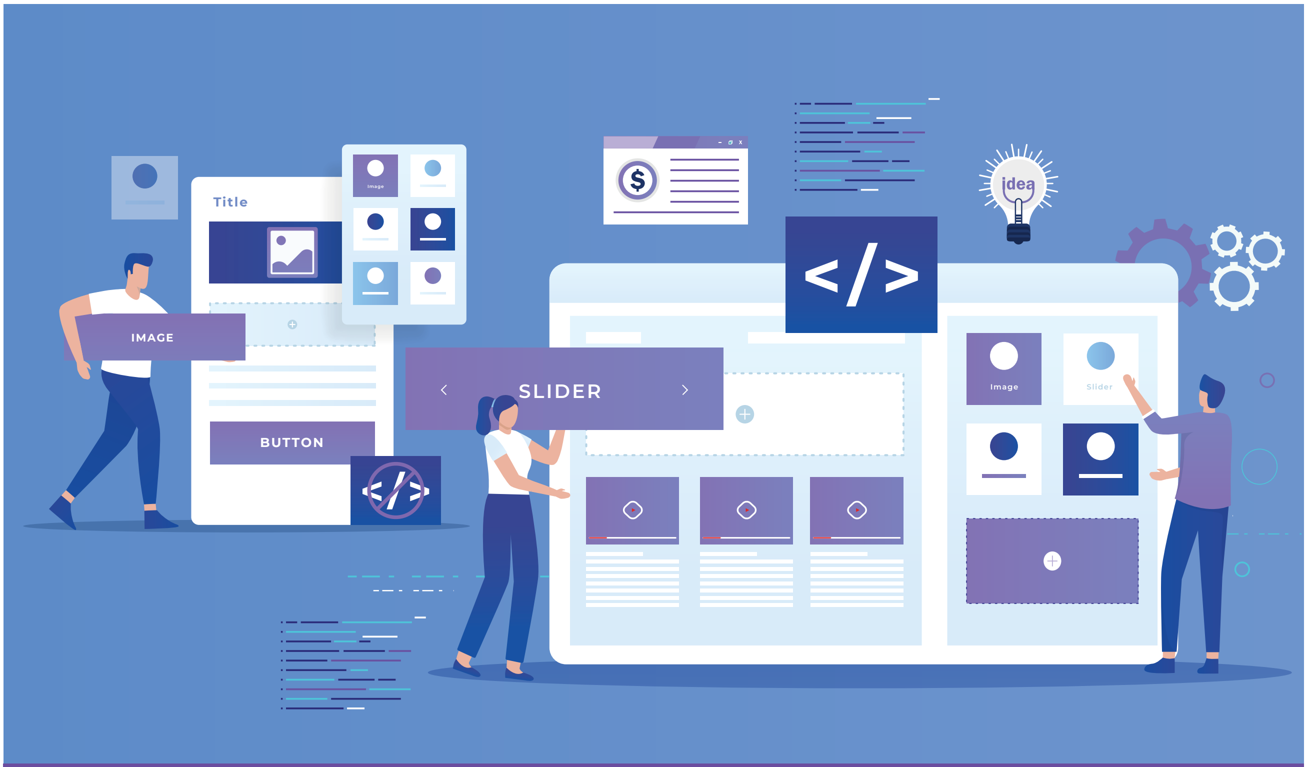
To address these challenges, CISOs must create security strategies and deploy solutions capable of providing scalable, integrated security that provides broad visibility and enables automated threat detection and response across their organization's security architecture.

This starts by deploying an expansive security platform designed to function seamlessly within and across different environments. This platform should serve as a central point of control for seeing, managing, and orchestrating a suite of fully integrated solutions deployed at every edge. And it should support common standards and APIs to connect existing solutions into a single security framework.

By converging networking and security, CISOs can ensure that dynamic changes to the network are automatically protected without impacting performance or productivity, ensuring the best user experience for employees and customers alike. A zero-trust access strategy helps ensure secure access to protected resources, identify unmanaged devices, and monitor for unusual behaviours across a highly distributed workforce. An adaptive cloud security protects applications and infrastructure in and across cloud environments, as well as extends security to users both on and off the network. When all of these systems are working together and sharing a common threat intelligence framework, real automation can be put into place to detect events, conduct an investigation, and coordinate a system-wide response without requiring human intervention. Which means your security team can focus on strategic solutions for DI initiatives.

Digital innovation and rapidly adopted realities like remote work have led to a complex and expansive digital attack surface that threat actors are taking full advantage of. By integrating security into every facet of the network, CISOs can ensure that their team dynamically adapts to challenges and remains agile in the face of adversity. Breaking down the traditional walls between network and security and creating a more integrated and automated fabric ecosystem should be top of mind for CISOs who need to be prepared for any eventuality in order to thrive in the new digital marketplace. ■

The author is Regional Vice President, India & SAARC, Fortinet



Low-Code And No-Code Platforms: Key Issues Enterprises Should Be Wary Of

Enterprises should bridge the knowledge gap before rushing for low-code and no-code platforms

By Jatinder Singh

Over the last couple of years, drag and drop platforms, also known as low-code or no-code platforms, have gained immense popularity amongst enterprises to build great applications for mobile and web and automate processes without any significant manual efforts.

While low code and no-code platforms aren't entirely a new phenomenon, the pandemic-driven dynamics have pushed many enterprises to extensively test these platforms to elevate customer experience and digitize company-wide operations. These drag and drop interfaces often come with AI and ML-based integrated applications, with built-in integration and databases, offering ready-to-use templates for enterprises who want to build applications and automate processes without engaging developers to write the HTML or iOS code.

A Gartner forecast projects that the worldwide low-code development technologies market is expected to reach USD 13.8 billion in 2021, primarily driven by the surge in the remote working model during the COVID-19 pandemic. Another study by Forrester anticipates that the no-code development platform market will grow from USD 3.8 billion in 2017 to USD 21.2 billion by 2022. These are massive projections.

Last year, Google acquired AppSheet to bring code-free development to the Google cloud and enable its customers to develop mobile apps without writing a line of code. This was considered a significant development since Google tried its hands in the no-code/low code solution offerings without much success. Other technology companies, such as Microsoft, Amazon, ServiceNow, Infosys, and HCL Technologies are rapidly building their low-code and no-code solution capabilities. All this indicates that the low-code and no-code platforms are now becoming mainstream.

However, many enterprises still fail to get the desired functionality they want from the low-code development ecosystems despite the excitement and massive growth projections. In the past, IT decision-makers who have rushed to deploy low code/ no-code platforms to accelerate their digital transformation journeys had to master their learning curve before reaping any significant advantages.

Limited availability of templates

Many vendors and solutions providers have been marketing their low-code/no-code tools as the simplest way of application development and workflow management, even when the company doesn't have enough technical knowledge or resources. IT decision-makers, however, need to consider various factors before immediately implementing these tools. One of the biggest challenges that codeless platforms have is the limited availability of patterns to choose from. Companies often design these pre-built app templates to create web and mobile applications with specific use-cases.

For years, many enterprises have been trying and testing the low-code and no-code platforms to solve the problems quickly and democratize the technology. These platforms have been beneficial for businesses that do not have the requisite budget...

Enterprises that need moderate to extensive customization should have the in-house talent to scale the applications. In low-code platforms, IT decision-makers should ensure that they have a certain level of coding skills to support apps' development. It is likewise essential to note that every tool has some constraints, and if you've not planned about the final result that you want to achieve, the chances of getting complex and costly workarounds when scaling up the app remain high.

Security and governance issues

For years, many enterprises have been trying and testing the low-code and no-code platforms to solve the problems quickly and democratize the technology. These platforms have been beneficial for businesses that do not have the requisite budget to hire software developers or outsourcing agencies to develop the necessary cloud infrastructure. While employees can quickly learn the deployment of these platforms, unlike custom development, these platforms may not give complete control to IT heads regarding security and governance issues. There are various risks involved, such as a no-code/low-code solution provider getting acquired by a third company or non-technical experts developing applications that may include critical customer data.

According to Forrester, currently, about 12% of enterprises manage their processes using low-code tools.

```
<!DOCTYPE html>
<html>
<body>

<?php
echo "<h2>PHP is Fun!</h2>";
echo "Hello world!<br>";
echo "This is PHP Language!";
?>

</body>
</html>
```

There are still many hang-ups since the investments in legacy systems have been on a higher side. Transitioning to pre-configured modules and functionality is also not without risks. Without any coding expert, the chances of putting insecure codes remain high, and sophisticated hackers can leverage that to obtain sensitive organizational data.

In the complex ecosystem of contending vendors, organizations must select a solution provider with foolproof built-in security capabilities. IT decision-makers should remember that even if they are using a third-party tool, the responsibility of securing the data lies with the enterprise. The vendor should provide the security certifications and necessary governance models to effectively run the no-code/low-code platform.

IT decision-makers should remember that even if they are using a third-party tool, the responsibility of securing the data lies with the enterprise. The vendor should provide the security certifications and necessary governance models...

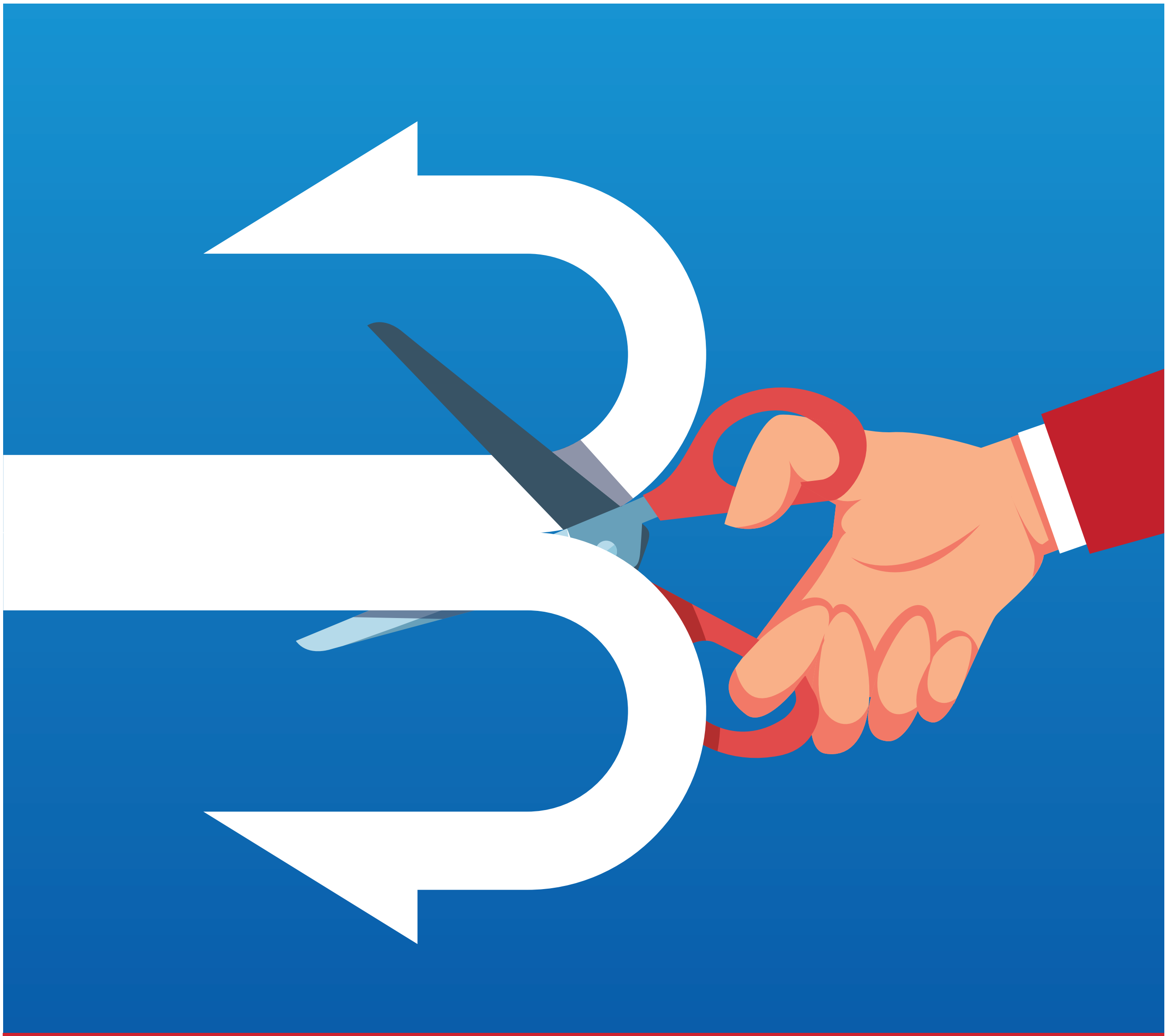
Scaling related challenges

One of the essential factors that IT decision-makers should keep in mind when choosing a low-code/no-code development platform is an in-depth analysis of application scaling. In most no-code/low code cases, the platforms become too stiff or restraining to accommodate desired functionalities promptly.

The majority of these drag and drop platform works exceptionally well in a small set-up with a limited set of users. However, the real challenge comes, especially in large set-ups when businesses want to scale. This is a common challenge faced by organizations and in-house developers. If more customization is needed based on user feedback, even the no-code or low code platforms have to be extensively built. Technology leaders must assess suppliers' ability to provide ready-to-use solutions when needed while scaling up software or internal client applications.

Most importantly, while picking a low-code/no-code partner, organizations should keep in mind that there could be a restriction of working with the larger firms, such as Google, Microsoft, and Salesforce. They may not allow application development processes beyond their environments. On the other hand, many other small solution providers may offer plenty of options to develop no-code/low code applications, even in the on-premises environment.

An ideal no or low code platform should enable the organization and IT decision-makers to achieve their business goals without compromising security while ensuring the functionality can be scaled up in case of a requirement. For a winning no-code/low code technology strategy, an organization needs to carefully analyze which platform they want to commit to and whether there is a precise alignment between business goals. ■



Could The Dell-VMware Spin-Off Be Of Greater Value?

The spin-off aims to enhance the unique capabilities of Dell and VMware in the do-from-anywhere economy. However, there are still questions that need answers

By Jatinder Singh

Dell Technologies' announcement to spin off its majority stake in the virtualization company, VMware, gives two perspectives: First, Dell's efforts drive greater efficiencies, innovation, and value for both its and VMware's enterprise customers. Second, its failure to achieve the desired synergies from its widely-publicized EMC deal.

According to Wall Street Journal, Dell's 81% stake in VMware is estimated at USD 52 billion. As part of the spin-off agreement, VMware would pay a special cash dividend of USD 11.5 billion to USD 12 billion to Dell's shareholders, including USD 9.3 billion to USD 9.7 billion for Dell. The financial restructuring will help Dell pay a significant part of its debt and strengthen its capital structure when digital transformation is high on the agenda and businesses plan higher investments in upgrading their technology infrastructure.

One may recall that Dell purchased 81% of the stake in VMware through the high-value acquisition of EMC (which purchased VMware in 2004) for more than USD 60 billion in 2016. Although the blockbuster deal was celebrated by many of its stakeholders initially, Dell and VMware soon found out that the merger was far from perfect and had no synergy.

A union that wasn't perfect?

The union of Dell and VMware had its highs and conflicts. Dell has co-partnered for several products around end-user computing, software-defined networking (SDN), hybrid cloud, and converged infrastructure with VMware. On the other hand, Dell and VMware could never reach a winning consensus on many of VMware's enterprise security initiatives.

VMware boasts of some of the exciting next-gen security solutions, such as Carbon Black and Workspace, which it has been keenly looking to integrate with its virtualization software platforms.

Additionally, before the pandemic, Dell's computer and storage products and the EMC storage unit were facing growth challenges through the U.S.-China trade war. As a result of this, Dell was unable to control its hardware component costs. At that time, many analysts claimed that Dell was leveraging VMware's research and development budgets to navigate the difficult times.

Why this matter for enterprises?

While Dell had been mulling about this spin-off (or a speculative reverse merger) for the last 18 months, the timing of the announcement couldn't have been better. Michael Dell is well aware of the growing opportunity and higher margins in the server business, helping him generate more significant business opportunities for VMware as an independent unit.

On the other hand, Dell is expected to use the spin-off transaction to reduce its debt and generate more value in the notebook PC business, the demand of which has suddenly grown exponentially, primarily due to increased work-from-home and study-from-home arrangements. Eventually, Dell can also focus on putting more robust efforts to strengthen its back-end servers, storage, and network infrastructure that are linked with the PC business.

As an independent entity, VMware, which is Dell's most profitable unit currently, stands a better chance to fulfil its vision in developing cutting-edge software and SaaS platforms across all clouds. After the spin-off, VMware will be better positioned to undertake its R&D efforts in enterprise security solutions and deliver better value to its enterprise customers.

"A spin-off from Dell Technologies provides VMware increased freedom to execute its strategy, a simplified capital structure and governance model and additional strategic, operational and financial flexibility while maintaining the strength of the two companies' strategic partnership," VMware said in a statement.

The statement adds that the spin-off will provide VMware with increased strategic, operational, and financial flexibility and agility to drive its growth strategy. This includes simplifying capital allocation decisions and eliminating the current dual-class stock structure.

> **One may recall that Dell purchased 81% of the stake in VMware through the high-value acquisition of EMC (which purchased VMware in 2004) for more than USD 60 billion in 2016**

On the face of it, it looks like the enterprise customers stand to benefit from the spin-off as the separated entities will be able to focus extensively on their customers and initiate specific research and development efforts to provide exceptional value to their users.

Both the companies, however, will continue to co-engineer solutions for enterprises, although through a newly defined commercial agreement.

It would be interesting to see if Dell would still depend on VMware's resources and research and development funds in the event of another crisis. Also, in areas such as enterprise security where VMware has high hopes, and Dell seems to be broadly interested in charting its own path through partnerships or acquisitions, will there be a change in strategy? ■

The No-Buffering Era Of 5G Will Make Live Videos Lively

With the growing demand for faster network speeds and reliable connections, there is a strong pull for 5G in the country

By Pankaj Gupta

The world is slowly yet steadily recovering from the havoc unleashed by the COVID-19 pandemic. At the beginning of the outbreak, businesses and people had to identify new ways to sustain their day-to-day activities during difficult times. The blessing in disguise were technologies, including cloud communications, which kept us connected and enabled remote working. Even as there is a strong hope today, that humanity will leave the deadly virus behind, one key learning for businesses is to be future ready by adopting communication technologies, which allow a contactless engagement with customers.

Given the scenario, businesses are increasingly inclined to deploy live high-definition video interactions with their customers and other stakeholders. Traditionally, the live video experience in India has faced issues, such as bandwidth crunch, inconsistent connections, etc. However, with the growing demand for faster network speeds and reliable connections with stronger bandwidth, there is a strong pull for the 5th Generation of telecom standards, aka, 5G, in the country and around the world. In fact, all the major telecom operators in the country have already expressed their readiness to test their 5G networks, subject to Government approvals.

Based on some global experiences, 5G will usher in a new, no-buffering era of data consumption. It does so by providing a 10x reduction in end-to-end latency. This gives the consumers the ability to enjoy seamless, immersive VR experiences, ultra-low latency live broadcasts, high-speed mobile video communications and so on. Furthermore, 5G also leads to a lower cost per gigabyte consumed, thus, making video calls more cost efficient.

Whether it's a retail environment, a power utility grid, or a healthcare facility, 5G can provide reliable data in real-time that can help an organization make better decisions

With 5G capabilities, cloud communications service providers have the opportunity to create rich experiences in live video communication between a business and its customers. Whether it's a retail environment, a power utility grid, or a healthcare facility, 5G can provide reliable data in real-time that can help an organization make better decisions. Because it can transmit so much information so quickly, a 5G network can gather and process data from multiple sources so people can actually see and address potential issues as they're happening rather than trying to determine what went wrong. In the financial industry, fintech firms can meet their Know-Your-Customer (KYC) guidelines by video calling their customers, eliminating the need for any physical presence at the local branch. Such use cases affirm that technology providers can ride the 5G wave to integrate real-time communication, i.e. video calling, into mobile applications and workflows, make physical meetings for day-to-day business interactions redundant and create a truly digital business world.

Given that 5G has already witnessed successful implementation in many countries in Asia, it is only a matter of time when India jumps on the wagon too. The impact of COVID-19—limiting face to face interactions but driving the digital adoption, will accelerate the rollout of more innovative and compelling live video conversation solutions to fill in the gap. The bottom line is that everyone should fasten their seat belts to embrace a lively world of live video meetings. ■

The author is CEO & Founder, EnableX.io

Can Artificial Intelligence Help Fight Pandemics?

Intelligent data and analytical solutions can help keep a vigilant eye on the emergence of pandemics and fortify healthcare supply chains, provided they follow diligent data processing methodology

By Jatinder Singh

The rising wave of the pandemic and the record number of cases has made it imperative for governments worldwide to identify innovative ways to track, detect, and diagnose COVID-19 cases and prepared for such a crisis in the future. Since the beginning of the outbreak, it has become challenging to track spikes in the coronavirus cases and predict their impact on the community.

The contagious virus resulted in uncertainty in every aspect of human life. And it has become soon evident that to tackle the gravity of the situation and be ready for such a future crisis, an extraordinary effort is required. In the last twelve to fourteen months, much research and analysis have been done on discovering the best ways to curb the coronavirus. However, even with stringent social distancing measures and accelerated vaccination programs worldwide, many countries are still struggling to prevent the alarming levels of virus spread and its severity.

In such a scenario, decision-makers are continually looking at technological interventions such as Artificial Intelligence (AI), Machine Learning (ML), and deep learning to make better predictions, act quickly, and minimize the impact of the pandemic. The AI-based epidemiological models have the potential to identify the possible hot spots of the disease swiftly and guide governments to accelerate health infrastructure and take proactive measures.

Today, millions of gigabytes of data and resources are available to track and identify pandemic-related patterns in a timely way. From infected patients' blood results to their age, sex, testing records, vaccination participation, treatment methodologies, availability of essential medicines and supplies, and outcome, a massive set of available data can help predict the future waves and analyze the overwhelming health care system. There are already some success stories, and many others are emerging. Data scientists are continuously evaluating the best ways to harness COVID-19 data using relevant algorithms and various simulations.

> While these tools are still at an early stage of development, soon they can play a substantial role in identifying the emerging patterns of infectious diseases and inform global agencies and authorities...

Early outbreak warning system

AI is no longer a marketing hyperbole. In recent years, deep learning and intelligent analytics have been effectively leveraged by companies and governments globally to accelerate production levels, analyzing disease patterns, and improve decision-making with a high degree of accuracy.

AI and ML have already proven their competence to detect an outbreak and even classify the locations that might need immediate attention. For instance, on December 31, BlueDot, a Canadian AI-based health monitoring platform, observed some strange pneumonia cases in Wuhan, China, using natural language processing and machine learning. Launched in 2014, the platform analyses over 100,000 news reports and studies about diseases in 65 languages every day. The platform analyses the data and consults with epidemiologists before sending warning signals.

The platform alarmed public health officials of several countries even nine days before the WHO released a warning statement around novel coronavirus. The same AI platform also identified India and Brazil as future epicenters months before the second wave hit in these countries.

Early outbreak warning systems are much needed to generate an immediate response and control the spread of COVID and impending epidemics. While these tools are still at an early stage of development, soon they can play a substantial role in identifying the emerging patterns of infectious diseases and inform global agencies and authorities to take proactive measures.

By scanning social media, different news articles, studies, and government data of various countries, these tools can analyze international data to forecast future events. While some of these AI systems can be fully automated, many others need constant human supervision to ensure that the correct data is being fed and recorded appropriately.

Tackling the outbreak

During the first wave, the focus of most of the countries was to detect the exposure, and hence contact tracing apps such as Aarogya Setu were launched to alert users about COVID-positive cases near them. There were few countries, though, which planned it much ahead to combat the crisis.

Taiwan, for instance, demonstrated its competence to leverage new-age technologies effectively to handle the outbreak and curb coronavirus transmissions early. It developed successful data intelligence templates to map the virus transmission and take proactive measures to contain it through AI and ML-led data analysis solutions and technology integration. By effectively collaborating with local technology research institutes and experts in automation and data science, the government of Taiwan unified its national health insurance database with the immigration and customs database.

The move helped the country tracked vulnerable and high-risk groups and ensured timely requisite measures to stop the community transmission. The AI-enabled algorithms helped the government improve the accuracy of COVID tests and enabled practitioners to analyze the impact the virus has made on the body organs of COVID patients.

With a growing focus on inoculation globally to curb the disease, countries like the US and the UK have leaped forward in using AI technology to meet the demand forecasting of medical essentials and supply chain management. Last year, UK's Medicines and Healthcare Regulatory Authority (MHRA) partnered with Genpact UK to deploy a machine learning software to capture the critical information regarding the adverse reactions of the COVID-19 vaccines. The software screens yellow card reports voluntarily

submitted by patients and doctors, which entails unusual or side effects after taking COVID vaccination or administering medicines.

Similarly, IBM is helping the US government and hospitals to manage the supply chains of vaccinations through its Watson Health Analytics software. The AI-based software has been instrumental in predicting demand and ensuring vaccines are distributed fairly without any hiccups. In India, companies like Accenture and Microsoft collaborated with the Indian government to launch an AI-Chatbot, MyGov Saathi, to provide correct and latest health updates around COVID-19.

India's Defence Research and Development Organisation (DRDO) recently unveiled an AI-focused secure web-based COVID detection application software solution, ATMAN. The AI-based diagnostic tool helps rapid identification and analysis of lung condition of a patient by scanning chest X-rays and classify the images into Normal, COVID-19, and Pneumonia classes.

Learning from COVID-19

The COVID pandemic surge and the health crisis activated have changed everyone's perception of how healthcare services need to function. Across the world, the focus on integrating technology and innovative solutions to improve healthcare services has accelerated significantly. If we specifically talk about India, where the second wave of the pandemic resulted in an acute shortage of oxygen, medical supplies, and isolation beds.

> Any gaps, stereotypes, or biases can present significant risks of giving misleading signals to enterprises, health officials, and the public. There are also concerns related to data privacy and security...

Such a situation could have been averted or controlled better if the country had built a database of confirmed COVID leads. Then, through AI-based platforms, infected patients could get verified information, tracked, and asked to share about their complications to receive timely help from the government.

India's National Digital Health Mission program aims to create a digital health database of the country's citizens and develop necessary technological tools to address its need to improve its outreach to provide timely health care services.

Nevertheless, AI systems aren't unblemished. And while they offer tremendous potential to classify new illness types and transform the overall healthcare system, their effectiveness depends on data accuracy. The AI-systems algorithms make inferences from the data that is fed to them. Any gaps, stereotypes, or biases can present significant risks of giving misleading signals to enterprises, health officials, and the public. Then there are also concerns related to data privacy and security, preventing many users from sharing their accurate data for AI interpretations, hence needing to be addressed.

Building accurate healthcare databases and integrating them with the national identity number of individuals can serve as the foundation for developing robust AI-based healthcare tools. Such actions can minimize future surges of COVID, help improve the quality of healthcare systems and prepare us better respond to such outbreaks. ■

Double Scoop

Two times the revelation

Ashwini Kumar

Group PMO Head - IT, RSPL Limited

MY FAVORITE AUTHOR

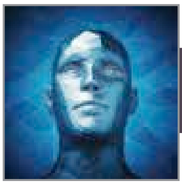
Robin Sharma

AN ACTIVITY I LIKE TO DO BEYOND MY PROFESSION

Reading Books

A TECH IDOL I ADMIRE

Elon Musk



AN EMERGING TECH WHICH WILL HAVE THE MOST IMPACT IN 2021

AI-ML

MY FAVORITE POLITICIAN

Atal Bihari Vajpayee

MY PEER IN THE IT COMMUNITY

Saikat Samanta, Head - IT, Videocon Industries

Saikat Samanta

Head - IT, Videocon Industries

MY FAVORITE SPORTSPERSON

Sourav Ganguly

A TECH JOURNAL I LIKE TO READ

SAP Journal

A GADGET WHICH I USE THE MOST

Smart Watch

MY FAVORITE CUISINE

Non-Veg Biryani

MY FAVORITE CAR

Honda City

गैजेट और टेक्नोलॉजी न्यूज़

To follow the latest in tech,
follow us on...

facebook.com/digitgeek

digit.in/facebook