Opinion | Pg 12
Automation And
Its Mistrusts

Insight | Pg 16
GDPR - Data Privacy
And The Cloud

ITNEXT

FOR THE NEXT GENERATION OF CIOs

THE CHANGING PAYMENT LANDSCAPE

And why it matters
for businesses—especially
consumer businesses

June 2019 | ₹100 | Volume 10 | Issue 01 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

WHO CAN APPLY?

You are invited to apply for the NEXT100 award if you:

- Have seven years (or more) of total work experience—after your under graduate degree
- Are currently employed full-time with an organization, and are resident in India
- Are managing the internal IT or technology team of your organization

WHY APPLY?

By participating in the NEXT100 process you get:

- Personalized personality and leadership analysis reports, for free
- Exclusive invitations to attend a variety of round table sessions and training workshops
- Become eligible to attend the CIO Masterclass program
- Opportunity to interact with India's leading CIOs and technology leaders

HOW TO APPLY?

To get started with the NEXT100 application process:

- Register on the NEXT100 award website (**next100.itnext.in**)
- Complete and submit the application between the notified open and close date
- Track and manage your application through a personalized dashboard

APPLICATION CLOSE
1ST JULY 2019

For details, please log on to
next100.itnext.in

INDIA's FUTURE CIOs
NEXT 100
2019
10 years
2010-2019

Note: 1. Valid documentation of educational qualifications, certifications and professional references will be needed for the evaluation process
2. There is NO fee for applying for the NEXT100 award

Age of the aware CIO

"What businesses are looking for are people who are extremely aware of what is happening around and can gauge if and how it would impact their business—either as a negative or positive disruptor"

Shyamanuja Das

There was a time when all that CIOs and enterprise IT professionals knew was technology. They were tech experts; knew how to implement tech when a consultant or a business guy told them what was needed.

With consistent campaign that understanding of business is a must, many of them today know their business processes and the pain points and try to provide the best IT solutions to support, run and close gaps in business processes. From tech implementors, they have evolved to become problem solvers. That's a great leap.

However, the approach is still the same. It is religious, ritualistic and no-point-wasting-time-on-what-is-not-there-in-the-syllabus approach. Ask them anything outside their business, you can draw blank stares. Some who have changed a couple of companies within the same vertical, have a slightly better view as they have seen different models and processes. But most of that knowledge has come from on-the-job experience.

Now, a selected few go beyond this limiting approach and do try to know what is happening in their industry and sector specific regulation. Yet, when it comes to even the issues that may impact their business directly, even though they are not strictly industry issues—for example, horizontal regulatory developments like data protection bill—many are not exactly aware.

In all these years, technology's role in business has increased manifold. Many businesses are being run on IT. Platform business models are impacting almost all industries—hospitality to transport, retail to financial services.

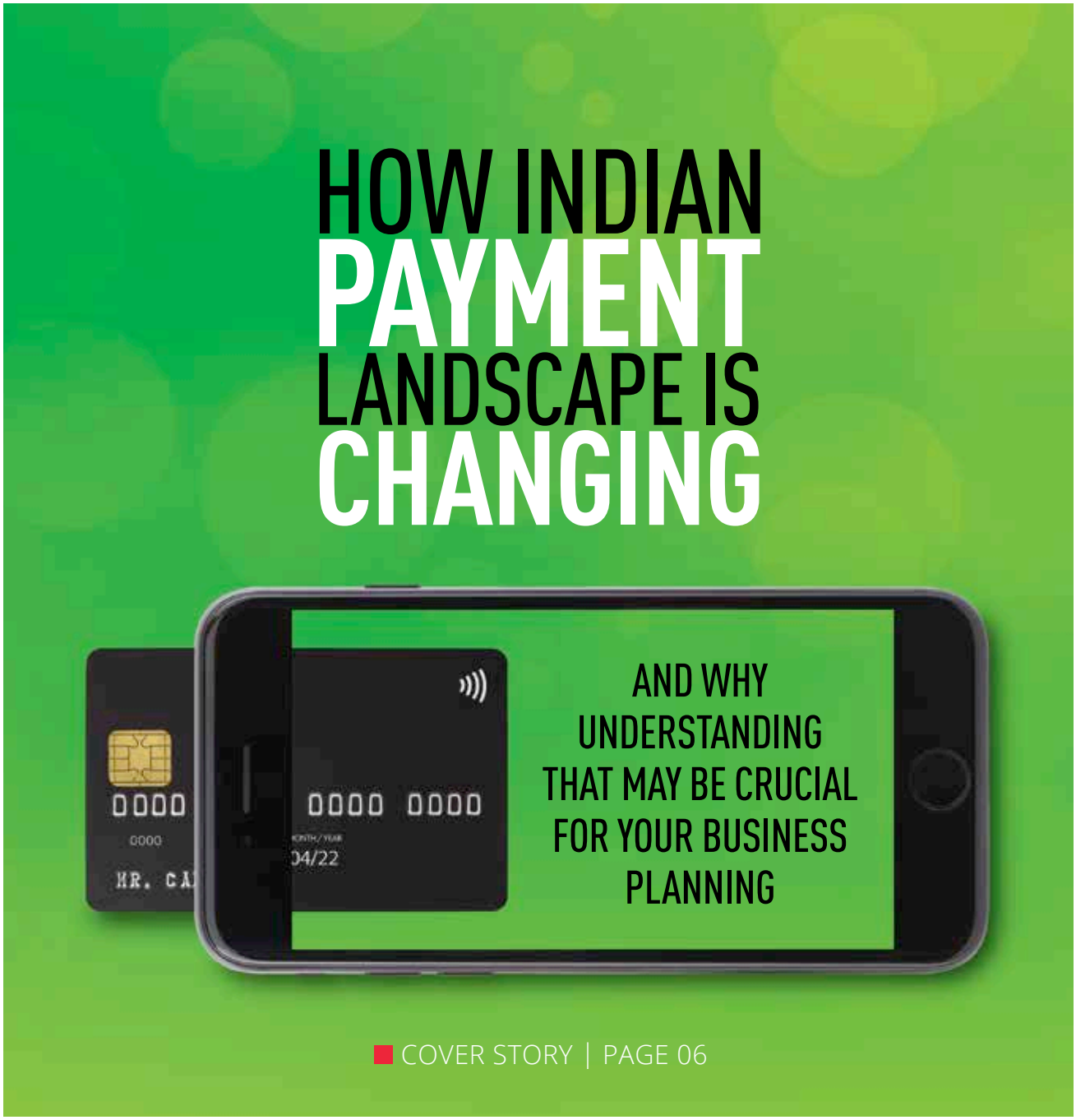
What businesses are looking for are people who are extremely aware of what is happening around and can gauge if and how it would impact their business—either as a negative or positive disruptor. That is, as a threat or as an opportunity. The next step of doing something about is actually much easier for today's CIOs. They exactly know how to solve problems.

This issue's cover story goes into one such 'peripheral' issue—digital payment—understanding of which can provide great scope for creating business value, especially to all consumer businesses. Digital payment is making it possible to create new products and services and take some of the existing ones to areas hitherto thought to be unreachable. On the other hand, the ease and convenience of digital payment, goes a long way towards enhancing customer experience.

But to turn this into a real business value creator, one must understand where exactly it is going and what can be expected. The cover story is just a little introduction to the area. Its objective is to create an interest in the topic—an essential part of any digital journey. ■

JUNE 2019
VOLUME 10 | ISSUE 01

Content



COVER STORY | PAGE 06

Cover Design:
BAIJU NV

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
Managing Editor: Shyamanuja Das
Assistant Manager - Content: Dipanjan Mitra

DESIGN
Sr. Art Director: Anil VK
Art Director: Shokeen Saifi
Visualiser: NV Baiju
Lead UI/UX Designer: Shri Hari Tiwari

SALES & MARKETING
Director - Community Engagement:
Mahantesh Godi (+91 98804 36623)
Brand Head: Vandana Chauhan (+91 99589 84581)
Head - Community Engagement:
Vivek Pandey (+91 9871498703)
Community Manager - B2B Tech: Megha Bhardwaj
Community Manager - B2B Tech: Renuka Deopa

Regional Sales Managers
North: Deepak Sharma (+91 98117 91110)
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
Manager - Events: 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

99 GROUP

EXTRA Curricular

Towards a sustainable future

Cleaning Up

NEXT100 Winner 2016 **Meetali Sharma,** Corporate Risk, Compliance & Information Security Leader, SDG Software India shares her passion for cleaning up the environment and driving the 'green' initiative...

It was in 2012 when we bought a beautiful holiday home at the foothills of Himalayas (Hartola, Uttarakhand) and found it was getting polluted from pesticides and plastic. It was then that 'Simply Natural Welfare Foundation' was born with an objective to save the Himalayas from pollution, save Himalayan Rivers, and provide education and good health for all.

We started this initiative in Hartola, which is a small village in Uttarakhand with a population of about 600 people. Through the initiative of "Clean Hartola, Green Hartola", the foundation is bringing awareness in the villagers. Every year, we run a day long extensive cleanliness drive (with school students). Plastic and polybags are collected in boxes and then sent downhill for recycling. The drive also includes plantation of trees like Deodar and Oak. This is done in collaboration with forest department, self-funding or through contributions received from family and friends. Educational material (books, stationary, pencil boxes, etc.) and eatables (biscuits, juice, etc.) are provided to students for their efforts.

Apart from this, villagers and school students are given environment education on a regular basis. Farmers are encouraged not to use fertilizers and urea and let the plants grow naturally and organically. Dustbins have been installed in various places all around the village to collect waste and recyclable material. We have also encouraged people to save water by capturing water though methods like water harvesting. Through these efforts we want to:

- *Ensure sustainable and equitable use of resources*
- *Prevent degradation of natural resources*
- *Conserve natural and man-made heritage*
- *Raise awareness about the link between environment and development*
- *Promote individual and community participation*

As told to Dipanjan Mitra, Team ITNEXT

Meetali Sharma

Snapshot

Meetali Sharma is Corporate Risk, Compliance & Information Security Leader at SDG Software India. She is NEXT100 Winner 2016. She has done her MBA from Symbiosis and BSc from Lucknow University. She also has a Professional Diploma in IT from NIIT and PG Diploma in Computer Applications from Madurai Kamaraj University.

Embracing Individual Social Responsibility comes at an early age and propels the many initiatives

Upping The Social Ante

NEXT100 Winner 2017 **Sudhir Madhugiri,** Executive Partner, Gartner shares his passion for working for the community and building an educational, cultural and social foundation...

Every time I hear CSR, I wonder why it isn't ISR – Individual Social Responsibility. I count myself lucky since for me, social responsibility germinated when I was in school in third grade. Our school had tie-ups with certain NGOs, one of them championing the cause of the visually challenged. Each year, there used to be a campaign for fund collection and the highest fund-raiser in each class would get a certificate. Thus, it was more of a competition for me than contributing towards the cause.

In one such fund collection drive, I lost out and was disappointed about not making the cut. Only when my parents and grandmother helped me decipher what the donations meant for a blind child and how my actions helped the institution and society, did I fully realize that I was not competing for a certificate, but was working for a noble cause! I am sure this was fairly a defining moment for me at the age of around ten that I haven't looked back since then. The purpose was clarified. Once you know the why, the how starts showing up in multiple avatars. Right through school, I worked for causes associated with the blind such as volunteering for their annual day, being a scribe for board exams and taking a few summer classes to junior kids. During college, I worked on initiatives associated with building civil infrastructure, health and hygiene. During my professional career, I have worked on various initiatives such as teaching basic computer skills to students in villages around Mangaluru, distributing food and clothes to destitute, volunteering in fund collection drive for the mentally ill, afforestation drives in coastal areas ravaged by/susceptible to tsunami and volunteering at a Cancer Hospital in Bengaluru managing patient admissions and discharge.

As I went about doing this, I slowly noticed a greater degree of fulfillment in supporting education causes than other social causes. Ever since then, I have been part of various community initiatives supporting education. I fund one braille kit per annum, volunteer in teaching initiatives in government funded schools and participate in building educational kits for students studying in government schools. Currently, I am supporting a team of educationists on building a project plan for a Science Center to be opened in a place about 100 km from Bengaluru. Aim of the project is to nurture scientific temper in kids from rural background. Hope to continue this journey and contribute in small ways to the society.

As told to Dipanjan Mitra, Team ITNEXT

Sudhir Madhugiri

Snapshot

Sudhir Madhugiri is Executive Partner at Gartner. He is NEXT100 Winner 2017. He has worked in various managerial and leadership positions at companies like Thomson Reuters, Wipro and Infosys. He has done his Bachelors in Engineering and PG Diploma in Management Studies.

HOW INDIAN PAYMENT LANDSCAPE IS CHANGING

AND WHY UNDERSTANDING THAT MAY BE CRUCIAL FOR YOUR BUSINESS PLANNING

Digital payments increase efficiency, greatly enhance customer experience and minimize revenue leakage. They are the most crucial enablers of a digital journey for a business

By Shyamanuja Das

Payment may seem to be one small component in the overall business and economic cycle. But in reality, payment is the moment of truth in any economic or commercial activity. Digital payments help an economy in many ways.

It makes the financial system far more efficient. By making the money move faster, it also enhances the efficiency of economy itself. It makes transactions transparent and easy to track—not just from the point of view of checking corruption but also from policy decision perspective. Finally, it makes access to essential services and products convenient for the common man, by removing artificial roadblocks that traditional transaction systems have created.

No wonder, an RBI-appointed High-Level Committee on 'Deepening of Digital Payments' headed by Nandan Nilekani—appointed in January 2019 to recommend ways and means of deepening digital payments and bridge any gaps that exist in the system—has in its report submitted in May 2019, recommended increasing per capita digital transactions by ten times in the next three years, by increasing the number of users of digital transactions by a factor of three, from approximately 100M to 300M in the corresponding period.

Digital Payment & Business

Payment is the culmination of a sales cycle. In a consumer business—where invoicing and payment are not too apart—payment is, in fact, business.

Hence, any business traversing the digital path today cannot ignore the criticality of digitalizing its payment options in order to make its transformation more effective. Digital payments help in achieving three critical objectives associated with transformation.

First and foremost, it transforms the customer experience. Payment is the last thing the customer (read consumer in a B2C business) is going to spend time about. By making it seamless, customer satisfaction is greatly enhanced. With the rise of electronic commerce—where digital payment is a pre-requisite (even if we erroneously call cash-on-delivery as e-commerce), the payment experience may make or break the business, especially where the payment is regular and periodic—like say bill payment.

Secondly, it greatly contributes to enhancement of efficiency of the business cycle. And finally, it greatly reduces the possibility of revenue leakage and hence results in a more effective revenue management.

With so much at stake, businesses—especially those helping them leverage technology—cannot take a mechanical approach to just 'enable' digital payments. Rather, they need to carefully plan their business—promotion, product customization and even warehouses—based on the digital payment trends.

This is what it means.

Say, in a village of 5000, ten people are interested in a video streaming services. With high speed data available, they can get that easily now. If you want to reach 1000 such villages, you are reaching 10,000 customers. But before digital payments came in, a provider had to either set up a costly collection mechanism or go through the mobile operators. Both being not-so-convenient an option for a smaller segment of target customers, the segment was ignored. With digital payment mechanisms, that neglected segment is a big opportunity now.

For consumer businesses to plan and promote well, they must even understand specific trends within payment. Tying up with card issuers may not give the desired results if people predominantly prefer mobile wallets. Similarly, trying to sell high value products through mobile wallet payments may not succeed. The fact that average value of transaction with a credit card is several times that of average value of transactions with a debit card has its own implications for planning sales—be it in finalizing rural/urban mix or tying up with card issuers.

Understanding of overall payments trends, how they are distributed among various instruments/mechanisms and how users of a particular mechanism behave while paying may provide crucial inputs to better business planning.

Apart from past data, the directions of payment regulations can give some visibility into how the payment trends may change over, say next 2 to 3 years.

The story essentially provides insights into such payment trends.

Indian Payment Trends, Circa 2019

That India—like the world at large—is moving towards digital transactions is not exactly news to anyone.

But only a deeper insight into the trends can give some realistic inputs valuable for business planning.

This includes data points, such as:

- The magnitude of overall growth
- Growth and share of various payment mechanisms
- The volume and value of transactions across each payment mechanism (which also gives average value of transaction)
- The pattern of growth over a period of time (we have taken five years)

Beyond pure data points, one needs to understand the veracity of perceptions and narratives in place. A wrong business decision based on a wrong assumption can be counter-productive.

Take, for example, the predominant narrative that demonetization kickstarted digital payment in India. In a decision which has been politically supported and opposed vigorously, only data can show the truth.

In an analysis in November 2017, one year after demonetization, we showed that demonetization, let alone initiating digital payment, had little impact on overall value of digital transactions, but it did significantly push up mobile wallet and debit card usage. In other words, demonetization did not impact depth of digital payments in India but significantly enhanced its breadth by expanding reach. We concluded that demonetization democratized digital payments—not a mean achievement in a country like India.

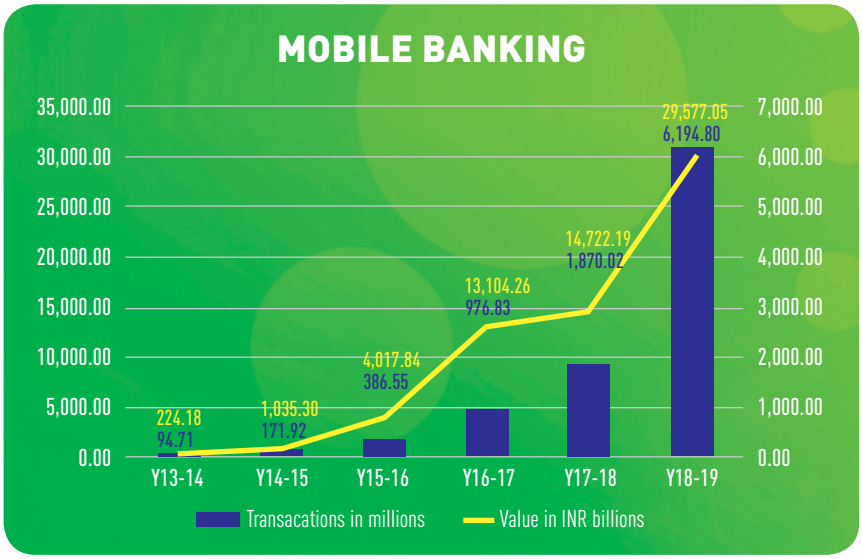
However, November 2017 was too early to gauge whether that impact was a lasting impact or an immediate disruption which was neutralized/regularized over a period of time. We will examine that now.

But it is not just demonetization's impact. There are other common perceptions that actual data analysis may dispel. We will get into some of them here.

For the purpose of analysis, we have taken RBI data on only retail electronic payments. So, no RTGS (real time gross settlement) or no paper clearing systems have been taken into account.

The payment mechanisms that have been considered are EFT/NFT, IMPS, debit card (point of sales only), credit card (point of sales only), m-wallets and mobile banking.

RBI's data for a five year period from financial year 2013-14 to financial year 2018-19 have been considered to better understand how the trends have evolved over the years.



Here are some of the insights payment data from RBI reveal—and what we could make out of them.

Overall growth in retail electronic payments over the five year period is 44% CAGR, supported by a strong, if not spectacular, growth of 39% in EFT/NFT which still accounts for 79% of the total retail electronic payments

All the newer form of payment—IMPS, m-wallets and mobile banking—have grown by over 100% CAGR in this five year period. So, people essentially are shifting to newer forms.

Mobile banking, which accounts for the second largest form of payment mechanism after EFT/NFT, has surprised everyone by growing 231% by volume and 101% by value in the single year 2018-19, on a much larger base than any of the other newer forms of payment. The buoyancy shown by m-wallets in 2016-17 on the wake of demonetization has cooled down in these two years. The segment, whose

size of transactions is just about 6% of mobile banking, has grown by a modest (by Indian standard) 69%.

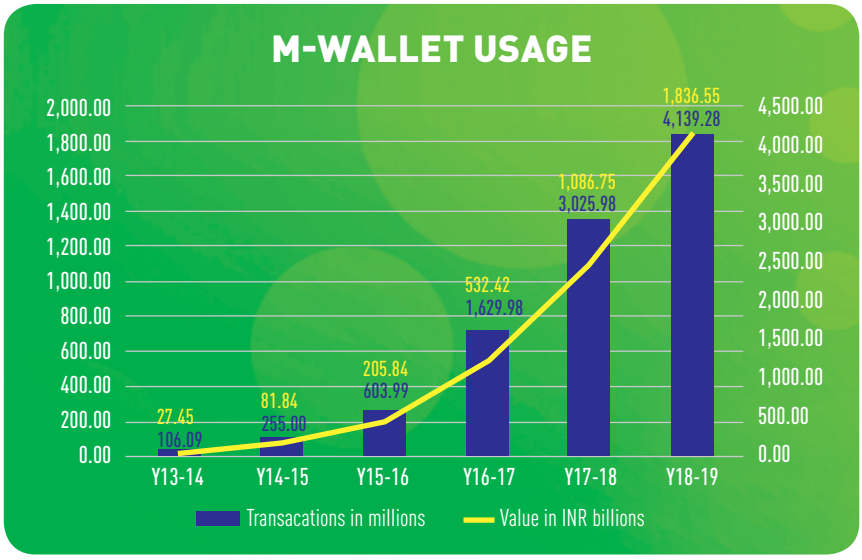
While it is understood that value of m-wallet transactions are smaller, what is surprising is that the number of transactions has shown an even lower growth—just 37%. The growth has steadily fallen from 170% in the demonetization year to 86% in 2017-18 and further halved to 37% in 2018-19.

So, what does this reveal? While no one can deny the role mobile wallets played in the two months after demonetization, it seems users have drifted away from mobile wallets, despite a number of mobile wallet players entering the business and some launching high profile marketing campaigns, supported by attractive promotional schemes like cashbacks.

While one section—having experienced electronic payment's benefits—have moved to a more mature segment like mobile banking which uses their bank accounts and does not block money in wallets, another, which was forced to use mobile wallets because of cash problems using demonetization and its immediate aftermath, seems to have gone back to cash.

A regulator-imposed upper limit in m-wallets may have impacted the growth of total transaction value in mobile wallets. However, it cannot impact number of transactions too negatively if the user base is growing and users are actually using it.

This—of users shifting most definitely to a more mature service like mobile banking from mobile wallets—is one of the most revealing trends which has implications for how consumer businesses should plan for their digital businesses.



Cards may not be as new a payment mechanism as some of the other digital payment methods—and there may not be as disruptive trends to notice. But the usage data of cards show clear and specific trends that are meaningful for business decisions.

Credit cards debuted much before debit cards in India. Yet, it has been restricted to a niche segment—thanks partially to lack of a robust credit rating mechanism and the aversion to 'credit' as a cultural issue among Indians.

Today, in a country of one and half billion people, there are less than 50 million credit cards. With many users being multiple card holders, the actual number of people who use credit cards may not be more than 25-30 million.

Debit cards, on the other hand, have been 'thrust' upon the banking users. Today, every bank ATM card is a debit card that can be used to pay using a PoS terminal at a merchant location. Yet, most use it as simply to draw cash from ATMs.

The two card instruments—credit card and debit card—though hyphenated often are two different animals.

Look at the contrast. More than 924 million debit cards in circulation in India accounted for just INR 5935 billion worth of transactions on PoS (excluding cash withdrawal from ATMs). Just 47.1 million credit cards were used to spend more—INR 6033 billion to be precise—by its users.

A debit card user makes an average payment of INR 550 a month while a credit card user makes a payment of an average INR 11900 a month!

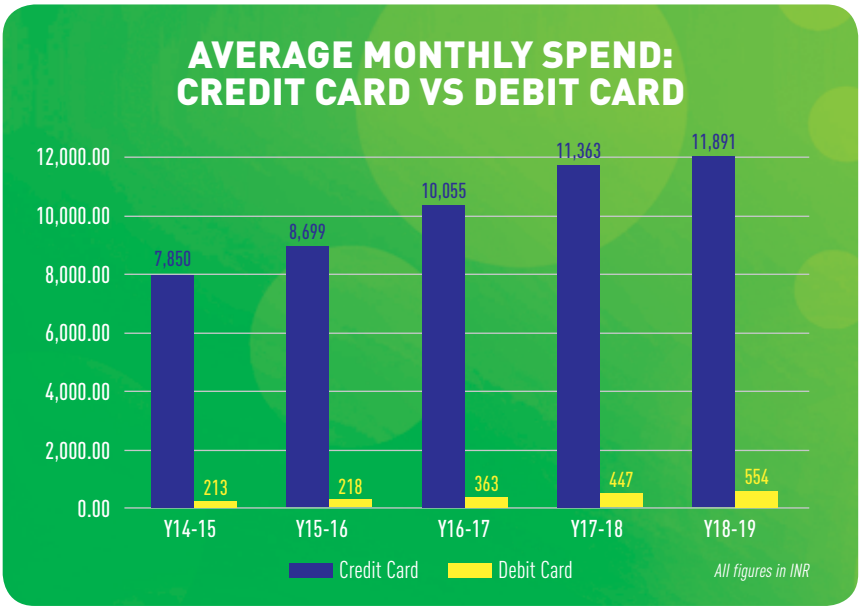
While growth of both has slowed down, debit cards got an impetus during demonetization. The instrument, which was showing an average growth of 30% before that, spent 108% more in the demonetization year 2016-17 as compared to the previous year, 20115-16. Credit cards did not witness any such spike.

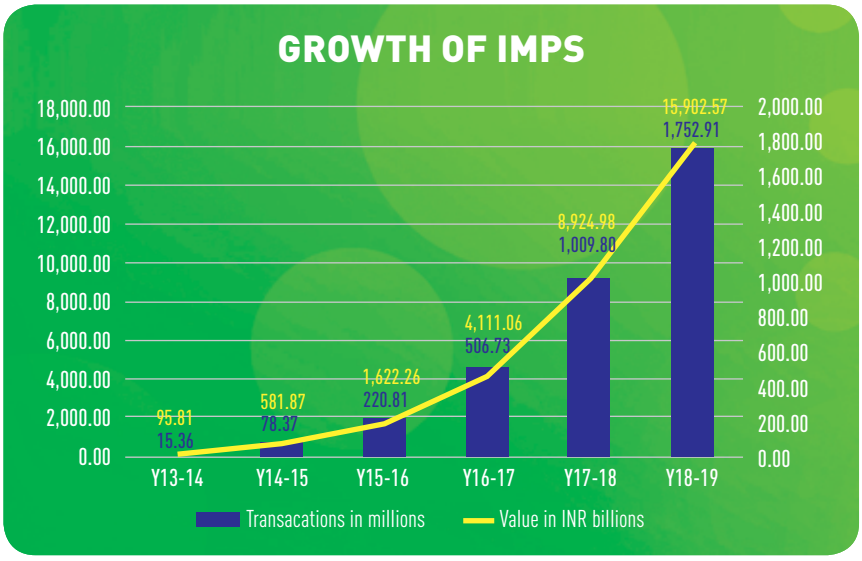
With India's new Payment Systems Vision 2021 clearly expressing an intent to move towards not just a less-cash society but also "to have a less-card India", cards have a limited shelf life. Card companies have already started virtual cards and are beginning to market them aggressively.

That brings us to IMPS—predominantly used for P2P transactions—which grew at a CAGR of 132% in terms of value in the five year period between 2013-14 to 2018-19 while showing a 108% CAGR in number of transactions in the said period. IMPS too accelerated during demonetization but not to the extent that mobile wallets and debit cards did.

Future Expectations

Contrary to popular perception, the surge in digital payments (even leaving out cards), did not start with either demonetization or Digital India. Reserve Bank of India has been following a very conscious and comprehensive plan to boost digital payments in India.





India's payment strategy is driven by its three-yearly payment systems vision statements. It is interesting to examine how the vision has progressed. In 2005-08, the vision was "the establishment of safe, secure, sound and efficient payment and settlement systems for the country". So, it was an intent, more than anything else.

The next vision document (2009-12) became bolder when RBI asserted that it wanted to "to ensure that all the payment and settlement systems operating in the country are safe, secure, sound, efficient, accessible and authorized". It was now no more an intent; it was a mandate it gave to itself as a regulator by promising to the nation that it (RBI) would make it happen. Also, with the UPA government focused on aam aadmi and social inclusion, financial inclusion as an idea was taking strong roots among policy makers. That thrust saw RBI adding "accessible" to its Payment Vision. It was sort of a passive intent towards inclusion.

That passive intent became a proactive stance in the next vision document (2012-15) as it added the word "inclusive" to the vision. But that addition was along expected lines. What was more noteworthy were the addition of interoperability and compliance.

The vision statement for 2018—the first after a new government took over at the centre, maintained continuity. It did not add any such new deliverables captures the implementation thrust quite unequivocally, by identifying the four pillars of achieving the vision of less-cash society. Two of those pillars—responsive regulation and robust infrastructure—were mostly about detailing of earlier plans or some augmentation in terms of specific tasks. Customer centricity was a new thrust but the document was devoid of any ground-breaking new plans or ideas there. The real takeaway of the 2018 vision was effective supervision. It was a mechanism for making the players—banks and other payment operators—more accountable and also more responsible, without RBI explicitly acting like a school master to ensure that each task is achieved.

In the time-tested way of RBI policymaking, the new payment vision 2021, released in May 2019, took the new idea introduced in Vision 2018—customer centricity—to make it the central focus of the new policy statement.

Vision 2021 concentrates on a two-pronged approach of, (a) exceptional customer experience; and (b) enabling an ecosystem which will result in this customer experience.

The Vision aims at:

a. enhancing the experience of customers
b. empowering payment system operators and service providers
c. enabling the ecosystem and infrastructure
d. putting in place a forward-looking regulation and
e. supported by a risk-focussed supervision

To achieve these goals, the Vision has four contours, it calls the 4 Cs–Competition, Cost, Convenience and Confidence. These four address innovative regulatory models like regulatory sandboxes for competition, efficiency through that competition helping reduce cost, better access to multiple payment systems and a

Reserve Bank of India has been following a very conscious and comprehensive plan to boost digital payments in India. India's payment strategy is driven by its three-yearly payment systems vision statements

no-compromise approach towards security that would enhance user confidence.

RBI has already completed a benchmarking exercise of India's payment systems with 20 other countries, identifying each aspect (41 indicators in 21 areas) of India's payment system as a leader (if ranked 1st to 3rd), strong (if ranked 4th to 9th), moderate (if ranked 10th to 15th) and weak (if ranked 16th to 21st).

According to that, India emerged as a leader across a dozen indicators. Those directly concerning with digital payment are:

- Regulation of costs of payment systems
- Number of debit cards issued
- Availability of alternate payment systems
- Share of e-money in the payment systems
- Citizen to government payment
- Business to government payment
- Government to business payment

India's payment system was found to be lacking (weak) in the following digital payment areas which RBI will address:

- Rate in decline of cheques
- Check volume payment
- Share of card payments in payment system
- People per PoS
- Value of debit card and credit card payments to cash in circulation
- Volume and growth of direct debits
- Share of direct debit in payment system
- Digital payment of utility bills
- Public Mass Transportation payment

While some of them such as cheque volume and decline of cheques cannot be addressed overnight, digital payment of utility bills can be significantly enhanced with right capacity building and policies.

In January, RBI had appointed a High-Level Committee on 'Deepening of Digital Payments' headed by Nandan Nilekani. The committee has already submitted its report in May. It has recommended a number of steps to RBI, government and businesses.

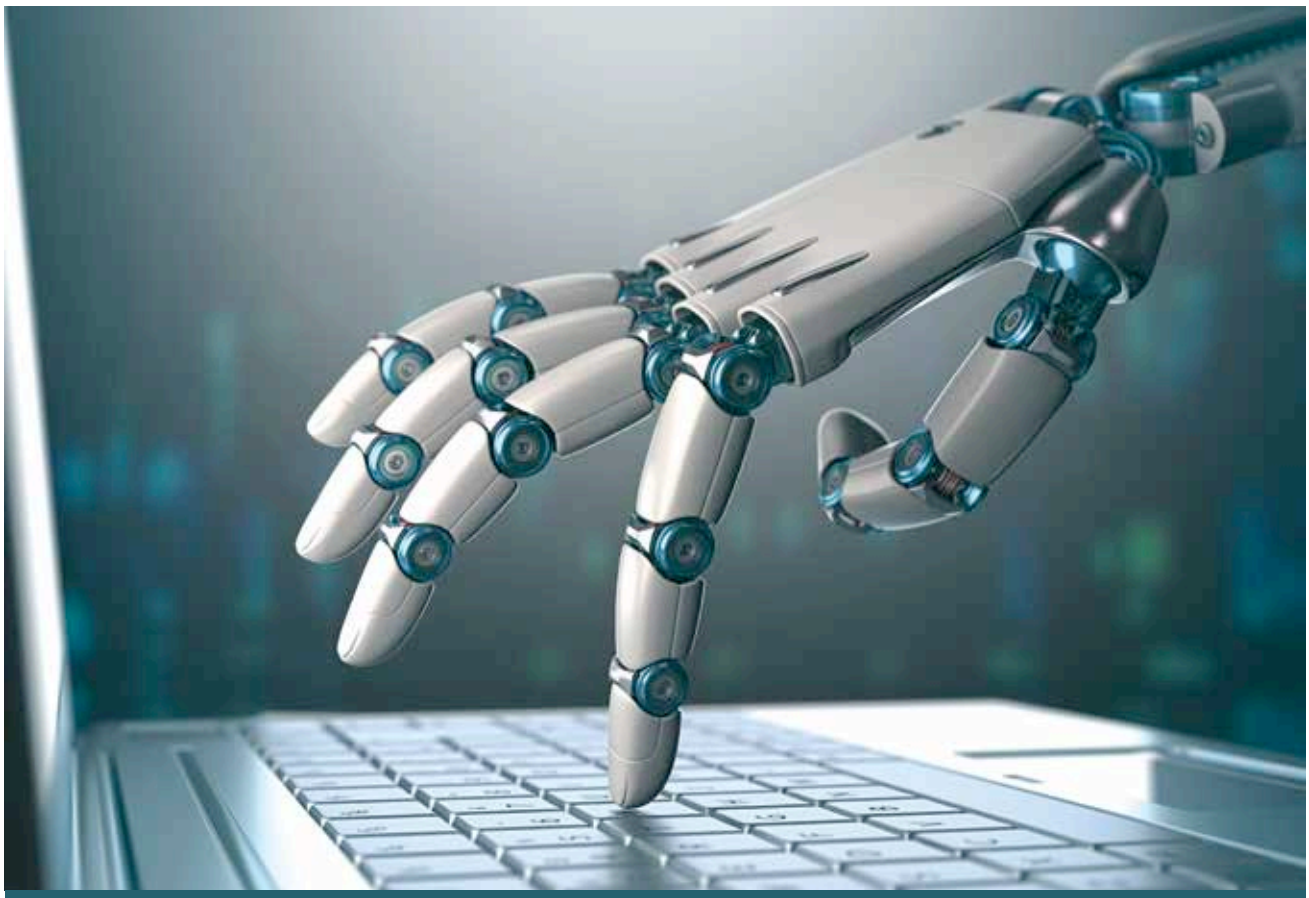
Some of the important recommendations include:

- Growing digital transactions volume by a factor of 10 in three years
- Better defining digital payment and strengthening data collection and tracking
- Addressing the issues of interchange fees and other issues in regular intervals
- Including non-banking entities in payment ecosystem
- Setting up of an Acceptance Development Fund to be used for improving acquiring infrastructure at Tier IV, V and VI areas, with contribution from card issuers and RBI
- Each merchant should support at least one digital mode viz BharatQR, BHIM UPI QR, or cards
- Allowing customers to initiate and accept a reasonable number of digital payment transactions with no charges
- Creating online dispute settlement systems by all payment operators including NPCI
- Continuous monitoring and improvement of transaction failures
- Operationalization of a FIN-CERT for oversight, and monitoring security of the digital payment systems
- Creation of a central fraud registry, that tracks all reported fraud
- Regular surveys to address digital payment issues and perceptions
- Promotion of digital transactions at rural farmer markets
- Promotion of interoperable standards for transit payments

In addition to these key recommendations, the committee has suggested capacity building, promoting digital literacy, tracking inclusion, enhance accessibility, use vernacular languages and similar initiatives to promote digital payments.

Businesses should expect some of these recommendations to become realities in next two-three years. It is advisable that they actively follow the real rollout on ground to get a realistic assessment of where digital payment is going. That will help them prepare better for the new real digital India, where the culmination of business—payment—is fully digital.

Real digital transformation strategies cannot ignore this most fundamental environmental change. ■



Automation And Its Mistrusts

The tech community should actively work to dispel the fears—and not just better the tools and technologies

By Shyamanuja Das

It is elections time and there has been huge uproar over the electronic voting machines (EVMs) as opposition accuses the government of manipulation.

But that is politics.

What cannot be taken lightly, however, is the statement made by former president Pranab Mukherji—considered to be a fair and reasonable person and a thorough gentleman—asking the Election Commission to ensure that there is no doubt in the minds of people.

"I am concerned at reports of alleged tampering of voter's verdict. The safety and security of the EVMs, which are in the custody of ECI, is the responsibility of the commission. There can be no room for speculations that challenge the very basis of a democracy. People's mandate is sacrosanct and has to be above any iota of reasonable doubt," said Mukherji.

Of course, the former president was not endorsing the opposition views that EVMs were being actively tampered. But he was urging the commission to act proactively so that whatever doubt that may be there in peoples' minds should be removed. Voting is the fundamental pillar on which democracy rests.

There are many who do not necessarily think that the EVMs are manipulated; yet, they doubt the efficacy of EVMs.

That is the mistrust with automation. If we have to progress, we have to do everything more efficiently and more correctly. Automation achieves that. So, progress gets seriously impaired if we avoid automation because of fear.

Not all fears of automation are about the transparency. Automation failing—and the failure creating a bigger negative impact—is an equally, may be bigger fear.

To err is human but to really foul things up requires a computer—the sentence of American biologist and population studies expert Paul R Ehrlich, beautifully captures this fear of automation.

Take a recent example. Delhi Metro Rail Corporation (DMRC) has been operating metro rail service in Delhi for more than a decade and half. And it has been appreciated for its management globally. On Tuesday, two trains were stuck on the track between stations because of a power failure. For two hours, the passengers were stranded inside the bogies without AC working. It was a nightmarish experience.

People were rescued, power was restored, and trains started running normally. It is a one-off incident in all these years. Normal trains and buses break down regularly. Passengers face a lot of issues. Yet, there is no fear of life. All they do is to get off and take an alternative vehicle. Some inconvenience, but there is no fear for life.

To err is human but to really foul things up requires a computer—the sentence of American biologist and population studies expert Paul R Ehrlich, beautifully captures this fear of automation

Yet, someone who has been traveling in Delhi metro every business day for more than seven years, took a bus today. The fear was very much writ on the face.

Automation, when it goes wrong, can really foul up things. In business tech too, one sentence that we keep hearing a lot these days is digitalization has made more and more parts of a business vulnerable. But the fact that everyone is going for it means the upsides are huge.

So, what is the way out? Today, those in charge of technology, try to make things better and the system more and more resilient and fault tolerant. That is their job. But they also have the onus of removing the fear from the minds of ordinary users. Just as the onus of creating trust on EVM machines lie with the Election Commission. ■

AI To Empower Workforce And Drive Objectivity

AI can help build a high-performance human resource team and as a result a high-performance workforce

By Mohua Sengupta

Corporate India is going through a defining time, with emerging technologies taking over many areas of business. Human resource is one such critical area, which is core to any business and has been going through rounds of revolution and transformation, both in terms of processes and technology.

AI happens to be the newest kid on the block, which is taking the recruitment processes by storm, as it is getting re-engineered every day, with more and more intelligent and repetitive work being replaced by AI. Let's look at some of the key areas where AI is being used to empower workforce:

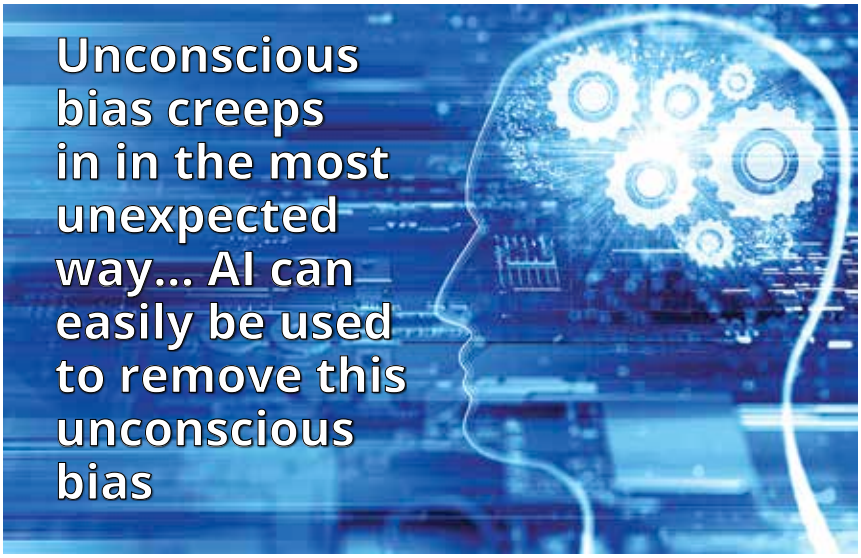
1) Removing bias – Unconscious bias is a huge challenge that all corporates are trying to fight. Corporate India is no exception. When it's a conscious bias, it's easier

to tackle but unconscious bias creeps in in the most unexpected way. It cannot only influence the choice of a candidate at the time of interview, but also the job description itself, making it a far more pervasive problem. AI can easily be used to remove this unconscious bias.

2) Evaluate profiles and first level interviews – Today sourcers and recruiters are spending a considerable amount of time in scanning, evaluating and shortlisting profiles and doing the first level interviews and the outcome of it is often very subjective, based on the emotional state of the recruiters. AI can easily take over these repetitive jobs, bring more objectivity to it and complete it much faster. There are quite a few AI-based platforms in the market today. According to a report by Forrester, by 2020, candidates applying to jobs at 20% of large global enterprises will interact with chatbots before recruiters.

3) Improved employee onboarding experience – Employee onboarding is the employee's first experience with an organization and it's the organization's best opportunity to create an excellent first impression. Today, due to a resource crunch and subjectivity associated with people, onboarding experience tends to be random and unstandardized. Using AI effectively can help new employees navigate their way into an organization more seamlessly, giving them an excellent onboarding experience.

4) Identifying the customised training requirement for employees – Mostly, people become redundant within an organisation because they lack relevant skills, but if we can train the employees in a timely fashion, then organizations can utilize its existing staff, without having to retrench and hire new employees. AI can be used very effectively to match existing talent with the required ones and identify the gaps in skillset and also to do a fitment of who is best trained on which of the required skills.



5) Resource management function – People intensive businesses have a huge challenge of finding the right skilled people internally at the right time and often end up hiring people at a higher cost, when an equally skilled person is available within the company. AI can help with this function and in a very time effective manner, thus reducing the cost of hiring, training and keeping a skilled resource on the bench.

6) Identifying people who are looking out – Losing trained and experienced employees to competition is a huge loss to any organization. AI can easily track the employees keystroke patterns, idle time & internet checking patterns and predict whether the person is looking out for newer opportunities.

7) Smarter and better people analytics – AI-enabled employee analytics provide the necessary insight to ensure better employee experience. It ensures meaningful employee engagement, creating happier employees and increased employee retention.

And these are only a few of the core functions that AI can do immediately. However, there still exists a degree of apprehension amongst the human resource fraternity to totally embrace AI, for reasons unfounded. AI today is not just efficient, it is also inexpensive. Just one word of caution, it is imperative that the recruitment processes are reviewed and reengineered to remove age old practices and made well suited for reaping maximum benefit out of AI. Research from PWC shows that 63% of companies are rethinking the whole role of their human resources department in the light of the impact AI will have on the business. Thanks to AI and RPA, human resource experts will be now able to focus on the core areas, which cannot be done by any technology. AI can help build a high-performance human resource team and as a result a high-performance workforce. ■

The author is EVP and Global Head of IT Services, 3i Infotech

GDPR - Data Privacy And The Cloud

Privacy regulations not only ensure that the PII of consumers is protected, but also raise the bar for security across the entire organization

By Rajesh Maurya

The General Data Protection Regulation (GDPR) which is celebrating its first anniversary, and the new India Data Protection Bill, provides consumers with added protection to ensure their privacy is safeguarded and prevents data theft or misuse. These legislations define what is meant by personally identifiable information (PII), establish compliance standards for organizations to meet, and impose penalties for organizations that fail to protect the PII of their customers.

Some of the most important benefits of these regulations is their uniform definition of exactly what is meant by personal data; detail rules for how that data can and cannot be used by any organization doing business within a specified region—or with any citizens that reside, work, or travel therein, even remotely; explicitly define what constitutes a breach of personal data along with standardized and consistent notification requirements; and give consumers complete control over the use and storage of their PII.

The GDPR established a common and broader definition of personal data than previous efforts, including things like IP addresses, biometric data, mobile device identifiers, and other types of data that could potentially be used to identify an individual, determine their location, or track their activities. The CCPA extends that definition even further, adding such things as geolocation data and shopping, browsing, and search histories.

Further, organizations affected by these regulations not only need to obtain explicit approval from individuals to retain and use their personal data, but also honour their "right to be forgotten," which enables individuals to demand that an organization purge any personal data about them for any reason.

Data Privacy and the Cloud

The challenge is that with today's highly distributed network, data could have been copied multiple times and distributed virtually anywhere. The recent and rapid transition to multi-cloud networks, platforms, and applications complicates this challenge. To meet data privacy requirements in such environments, organizations need to implement security solutions that span the entire distributed network in order to centralize visibility and control. This enables organizations to provide consistent data protections and policy enforcement, see and report on cyber incidents, and remove all instances of PII on demand. Achieving this requires three essential functions:

1. Security needs to span multi-cloud environments. Compliance standards need to be applied consistently across the entire distributed infrastructure. While privacy laws may belong to a specific region, the cloud makes it easy to cross these boundaries. Policies and protections established for data in a physical datacenter under the control of local privacy laws need to follow data as it moves to the cloud or to other datacenters as long as they are stored in the same geography. This creates two issues that need to be addressed:
   - The first is that you need a mechanism in place to keep track of every instance of that data, especially as it moves into and across multiple applications and workflows. Data has a tendency to multiply and you need a way to manage that information.
   - The second is that you need to ensure consistent segmentation across the entire distributed infrastructure. This becomes a challenge when security policies are confined to specific physical and cloud environments, and security solutions deliver inconsistent enforcement and functionality due to the unique requirements of different cloud environments. Security tools need to natively integrate into cloud platforms in order to consistently segment the multi-cloud environment, and policies need to be translated on the fly to accommodate differences in cloud platforms as data moves. And datacenters in other parts of the world need to support these new security requirements or they risk becoming the weak link in the security chain.

> The challenge is that data could have been copied multiple times and distributed virtually anywhere

2. Data Loss Prevention is essential. Tracking and managing PII requires the implementation of Data Loss Protection (DLP) technologies that can be applied inline as well as at the cloud API level. Such solutions need to be able to identify, seamlessly track, and maintain an inventory of all PII. A few key principles when it comes to handling and exchanging PII:
   - DLP monitoring needs to begin at the point of acquisition or creation of any PII data.
   - Data containing PII that is in use by applications or users needs to be monitored to be sure it is being securely accessed and processed.
   - Data in motion needs to be protected, especially when it is being transferred between different applications or cloud environments.
   - Data at rest, whether in the cloud or in a physical location, needs to be monitored and secured.
   - DLP also needs to track multiple versions of that data—or even pieces of that data—if they are copied, used by different applications, and stored in different locations.
3. Compliance reporting requires centralized management. Compliance reporting needs to span the entire distributed infrastructure. As with other requirements, this also demands consistent integration throughout the cloud and with the on-premise security infrastructure. Achieving this requires the implementation of a central management and orchestration solution, such as a SIEM or other single-pane-of-glass management console which has visibility to the entire multi-cloud & security infrastructure. What you don't want is having to hand-correlate data from multiple systems, because things get missed, and if they are found in an audit, the penalties can be severe.

Replace Reactive Solutions with Integrated and Proactive Strategies

The best approach to security is to stop an attack before it even starts, and limit its scope once a breach occurs. This requires organizations to have technologies and policies in place, such as:

- Advanced prevention and detection tools, including live threat intelligence, hardened access controls, behavioral analytics, and ATP solutions that allow them to get out in front of breaches.
- Intent-based network segmentation, including both network and micro-segmentation, to limit the impact of a breach to a specific data set or network segment.
- Tightly integrated security solutions that talk to each other, share threat intelligence, and coordinate a threat response. These tools also need to be natively integrated into the API infrastructure of the various cloud environments being used, allowing you to enforce policies and respond to breaches consistently across the entire network.
- DLP solutions that allow you to track data and prevent its unauthorized access, use, or transfer regardless of where that data is used, travels, or resides. Important for these solutions to be sharing information across the various protected infrastructures.
- Centralized controls that provide a single point of visibility & control for all data, ensuring that policies and configurations are consistent, breaches are detected and reported, consumer requests are honoured, and compliance reporting is consistent and comprehensive.

When properly understood, privacy regulations not only ensure that the PII of consumers is protected, but they also raise the bar for security across the entire organization. It forces organizations to go back to the drawing board, rethink processes and policies, identify and close gaps, and centralize their visibility dashboard feeds and operational controls. Many of these security fundamentals have been lost in the rush of digital transformation, and this is a good excuse to regroup, rethink, and re-secure your infrastructure. ■

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

Digital Transformation Efforts Fail Without Data Literacy, Shows Study

Organizations should hire Chief Data Officers (CDOs) to build a culture of analytics and encourage data literacy across the enterprise as part of their digital transformation strategy

As the data landscape becomes more complex, it is important for IT to unleash its potential to drive meaningful business impact. However, a new study reveals that approximately 54 million data professionals (including CIOs and data scientists, et. al) around the world face common challenges associated with the complexity, diversity and scale of their organizations' data. As a result,

most digital transformation efforts remain unsuccessful.

The study done by data analytics firm, Alteryx and IDC Infobrief, states that in an increasingly data-driven world, over 80% of organizations now leverage data across multiple organizational processes, but CIOs and data scientists still waste 44% of their time each week because they are unsuccessful in their activities.

The study further shows that CIO and data specialists spend more than 40% of their time searching for and preparing data instead of gleaning insights. On average, they use four to seven different tools to perform data activities, adding to the complexity of the data and analytics process. They also leverage more than six data sources, 40 million rows of data and seven different outputs along their analytic journey.

More than 30% of data workers say they spend too much time in data preparation, a task that can often be automated

CIOs' Data Woes

The top frustrations cited by data specialists are indicative of root causes that are responsible for inefficiencies and ineffectiveness. For example, more than 30% of data workers say they spend too much time in data preparation, a task that can often be automated.

The other problem is, eight out of 10 data workers, approximately 47 million people worldwide, use spreadsheets in their data activities. Spreadsheet functions are often used as a proxy for data preparation, analytics and data application development tools but are error-prone and expose the organization to compliance and trust issues.

"Data is at the core of digital transformation, but until organization leaders address these inefficiencies to improve effectiveness, their digital transformation initiatives can only get so far," said Stewart Bond, director of data integration and integrity software research at IDC.

"Consolidating platforms and looking for tools that address the needs of any data worker, whether a trained data scientist or an analyst in the line of business, can help reduce the friction that many organizations experience on their path to becoming data-driven," says Bond.

The survey also found that IT managers or data specialists are unsuccessful for a variety of reasons, including lack of collaboration, knowledge gaps and resistance to change.

Participants reported the lack of creative and analytic thinking, analytic and statistical skills, and data preparation skills as the highest-ranked skills gaps responsible for productivity issues, indicative of the pervasive talent gap that exists between data scientists and data workers in the line of business.

Can CDOs Reduce the Gap?

To overcome these issues and more, organizations should hire Chief Data Officers (CDO) to streamline analytic processes, build a culture of analytics and encourage data literacy across the enterprise as part of their broader digital transformation strategy, the study says.

Earlier, researchers pointed to the benefits of companies that have a dedicated data chief. Businesses that have a CDO are twice as likely to have a clear digital strategy, a 2018 KPMG study found. And two-thirds of such firms say they are outperforming rivals in market share and data-driven innovation, according to a recent IBM study.

"Collecting data alone won't digitally transform a business and the answer is not as easy as hiring a leader, a few data scientists or over-investing in disparate technologies. The key is to empower all users, many of whom are currently stuck in spreadsheets, to analyze data effectively to drive real, business-changing results," said Alan Jacobson, chief data and analytics officer (CDAO) of Alteryx.

Jacobson also notes that the CDO has to become the key ally to the CIO for accelerating the development of data driven businesses.

While there were several debates earlier if CDOs' role can eclipse that of CIOs in the organization, analysts believe in the age of collaboration, such discussions are passé. Instead of seeing the CDO as one more encroachment on its territory, IT should align with CDOs, influence their vision, support and enhance their projects, and make business sense out of the data. ■

Extravagance To 5G Game Change

5G is poised to be at least ten times faster as compared to 4G, and significantly more agile than its predecessors

By PM Dutta

Next-generation of 5G wireless systems are bringing about a prolific change in the telecom industry, enterprise and consumer space. Considered a scintillating 'hype' until recently, today, it is fast becoming a reality, as many countries across the world – including India – are already investing in 5G (or are planning huge investments in the near future) in order to gain from its intrinsic high-speed network and reliability lustre.

A recent research note by two US tech analyst firms, 451 Research (focused on the technology segments of business of enterprise IT innovation) and Vertiv (provider of mission-critical infrastructure technologies) has polled over hundred global telecom trend makers with meta visibility into 5G strategies and plans, endorse that enterprises were overwhelmingly optimistic about the 5G business outlook and are moving forward aggressively into deployment plans.

5G is poised to be at least ten times faster as compared to 4G, and significantly more agile than its predecessors. 5G is expected to steadfast hundred times more devices than 4G grid, giving rise to a deluge of concurrent IoT-enabled gadgets and devices. The evolution of 5G should certainly be of interest to C-level executives. The demand to upgrade the invocation metamorphism depends upon the core technical genre in order to comply with the twister of an ultra-fast future.

The reason for optimism among businesses is that they could benefit from more real-time online interactions with customers, have seamless video conferences with staff, and have a more well knit efficiently managed and connected network for real-time interactions and run intricate resource hogging applications — a fluidic 5G envelope poised to resolute the most critical business app's and improve bottomline outflow.

Service providers are also on upbeat, as 12% of operators expected to roll out 5G services by end of 2019, and an additional 86% expected to be delivering 5G services by 2021, according to the study. Chipmakers like Qualcomm and MediaTek have already announced the availability of 5G-enabled handset device this year. In the US, service providers like AT&T and Verizon have started deploying 5G networks. Ericsson has already announced several deals with global customers. In India, the government is determined to make a nationwide 5G rollout.

The survey encompasses most of those initial services will focus on supporting existing data services. About one-third of respondents expect to support existing enterprise services with 18% expected to deliver sublime enterprise services.

The Telco Readiness

As coverage expands, 5G itself will become a key enabler of emerging edge use cases that require high-bandwidth, low latency data transmission as virtual and augmented reality, digital healthcare, and smart homes, buildings, factories and metros.

Encompassing the scale of the challenge, near 68% telcos in the survey are sceptical about achieving total 5G coverage before 2028 or even later. 28% expect to have total coverage by 2027 while remaining 4% expect to have total coverage by 2025.

Hatching of 5G has a huge opportunity in India, further revolutionizing the app's and content ecosystem in this mega opportune. The global telco's have recognized this potential of network transformation which is required to render these state-of-the-art services.

The gruesome grits of the 5G services, telco's are ramping up the deployment of Multi-access Edge Computing (MEC) sites, which bring the capabilities of the cloud directly to the radio access network. 37% of the shares believe to have already deploying MEC infrastructure ahead of 5G deployments while an additional 47% gearing to deploy MECs.

As these new computing locations ground on fifth generation (5G) online, the ability to remotely monitor and manage increasingly meshed networks becomes more critical to maintaining revenue earns. In the area of remote management, Data Center Infrastructure Management (DCIM) was identified as the most important enabler, followed by energy management. Remote management will be critical, as the report suggests the network densification required for 5G could require operators to twice the number of radio access locations around the globe in the coming 10-15 years. Gartner report released in 2018 envisages a lack in readiness among telco's and communications service providers (CSPs) to an extent of 66% to deploy 5G by 2020, The CSPs' 5G networks are not available or capable enough for the needs of organizations.

In fact, telco's are also increasing network energy (electrical) consumption. The study shows AC to DC conversions loss will be an area of emphasis and significant concern to all telco's. Besides, new EER (energy efficiency ratio) cooling techniques will see the biggest jump in adoption over the next years of transition. Off late, the EER synchronizing is being used by 43% of the global telco's. This number is expected to increase to 73% in the coming five years from upgrades from VRLA (valve-regulated lead-acid battery) to lithium-ion/ polymer batteries showing a positive growth gradient of 66% as the telco's are upgrading their batteries. Five years from now, that gradient is projected to jump to 81% or more to reach to the point of inflection.

The 5G Challenge

It is clear now that 5G network bandwidth and speed will facilitate a surge (network tsunami) in high-bandwidth and real-time communications in corporate world, it's going to have an absolute impact on IT strategic plans. This will be challenging unless telecom companies have a strong digital strategy in place to leverage the impact.

Harnessing the chrome of intelligence and the 5G connectivity, wireless connectivity should be incorporated into the business plan. A Gartner report notes that IoT communications remains the most popular domain 5G, with 59% of the organizations expecting 5G-capable networks to be widely used for this purpose. The next most popular use case is 8K+ video – 53% of the downstream users per se.

Invocating 5G is going to affect the overall communications infrastructure in a converged technology medium and the focus on wireless infrastructure as a way of managing infrastructure for their Wi-Fi network and cellular devices as accorded in the OPEX cost. The foray of 5G base stations need to be much more densely deployed and the form factors have to be shrunk dramatically. In the US, several stadiums and train stations are integrating wireless LAN and cellular to offer a better user experience. The intrinsic use of the different service layers needed to support the many new sensors protocols in 5G applications need a strategic conceptualization. Ceteris paribus, a review/audit of the present network infrastructures is a prerequisite to understand what upgrades or replacements to network hardware, software, and services will be required to get ready for the 5G network upgrades that will have a deep impact to OPEX budget.

Findings from Ericsson reveal 3.5 billion IoT device demand will be there by 2023 — equalling five times the number of connected devices used now. Additionally, the company forecasts that 5G networks will spur the growth of Internet-connected devices. The enterprises should filter and accept only kind of data and exclude the rest from network access. This requires rigorous data planning to ensuring newer enterprise systems are being designed with a natural migration path to software-based systems to significantly reduce carbon footprint, fossil power, and cooling requirements while operating more of a datacenter software.

The transitioning to 5G will have its own security risks. Experts point out that 5G and the various new applications that will come will widen the arena for cyber criminals. A team of researchers discovered 5G security protocol, known as Authentication and Key Agreement (AKA) – a standard associated with a communications protocol organization called the 3rd Generation Partnership Project (3GPP). A poor implementation of the current standard can result in very serious security implications, unless organization work out a resilient yet stringent security measures while adopting a blue-print to 5G technology rollout.■

The author is Senior Manager - IT at Balmer Lawrie & Co

How AI Can Fuel Greater Innovation In The Enterprise

A new study by Microsoft and IDC shows that by 2021, AI will more than double the rate of innovation in organizations and in employee productivity in India

By Sohini Bagchi

In recent years, artificial intelligence (AI) has become a hot topic of discussion in the enterprise. With a flurry of AI advances, investments and new announcements that have taken the digital world by storm, businesses are betting big on AI innovation to better serve their customer, improve RoI and beat market competition. A new study by Microsoft and IDC Asia/Pacific, shows that by 2021, AI will more than double the rate of innovation at organizations and employee productivity in India. It is therefore imperative that CIOs and other leaders in the organizations begin to prepare for its impact now, so they do not fall behind.

The study, 'Future Ready Business: Assessing Asia Pacific's Growth Potential Through AI', conducted through a survey of 1,500 CIOs and business decision makers in mid and large-sized organizations across 15 economies in the region, highlights that those companies that have adopted AI expect it to increase their competitiveness by 2.3 times in 2021.

AI Innovation Success

Going by AI innovation use cases across enterprise, Microsoft highlights the case of ICICI Lombard, a private

sector general insurance company in India that deployed AI to process vehicle insurance claims and renew policies more efficiently.

"We recognized the potential of AI in providing high quality car damage evaluation services. With data being generated at an exponential level, this technology will help us derive insights to inspect and process claims with utmost efficiency. Using Microsoft's AI expertise is helping us bring about this transformation, allowing us to meet customer demands quicker without compromising on service excellence," informs Girish Nayak, Chief – Service, Operations & Technology, ICICI Lombard General Insurance Co.

According to Nayak, until recently, the sector relied on traditional ways to renew lapsed policies or address claims. Both services require inspectors to physically look over vehicles and make damage assessments. But with more than 230 million vehicles and 1200 auto accidents every day across the country, getting those inspections done and receiving approvals is time intensive, creating issues for both parties.

With the help of the AI-enabled app, in case of lapsed policy instead of a physical inspection, customers can simply take images of their vehicle and upload them with Insure. The app then uses AI and machine learning to divide the images into frames and identify the various parts of the car to look for damage. In most cases the AI module can make a judgment very quickly, reducing the time from days to just minutes.

"This has made life simpler for customers as they can file claims conveniently and receives estimates or approvals much faster than before. Further, automating the process reduces the possibility of inaccurate assessments due to human error as well as increased efficiency and productivity improves the bottom line. From the perspective of AI augmenting human capability, the role of the human insurance inspectors is changing as well, since AI is quickly handing the routine claims, allowing the company to attend to more complex claims where human intervention is required," he says.

Another example is Apollo Hospitals which is using big data, machine learning and AI areas of prediction, prevention and treatment. Apollo Hospitals' AI model helps gauge a patient's risk for heart disease and provides rich insights to doctors on treatment plans and early diagnosis. This was visible especially in the cardio vascular department, where nearly 3 million heart attacks happen in India every year and 30 million Indians suffer from coronary diseases.

Sangita Reddy, Joint Managing Director, Apollo Hospitals, says, "With AI deployment, now, when a patient goes for a cardio health check the doctor can do two things previously left to intuition. Firstly, they can build up a more accurate cardio-vascular health profile of the patient based on machine learning of all their previous patient data. Secondly, the doctor can make a patient health plan that addresses these possibilities whether it be prescribing medicine or recommending specific lifestyle changes."

Culture and Skillsets Essential

Despite some of the success stories, there are a number of challenges for companies to unlock the full potential of AI. Dr. Rohini Srivathsa, National Technology Officer, Microsoft India, states that in order to fully embrace tech intensity, organizations will also need to invest in their human capital.

"The rise of AI means that there is a necessity for workers to reskill and upskill to remain relevant and play a part in the workforce of tomorrow. In addition, CIOs and business leaders will need to drive cultural transformation within their organizations that values experimentation, agility, proactiveness and a growth mindset," she says.

The study clearly shows that while 85% of businesses are willing to invest in skilling and reskilling of workers to create an AI-ready workforce, 65% of them have yet to implement plans to train their workers. Technology leaders must influence on the urgency to invest in workers' training, as AI cannot progress without skilled individuals.

The study evaluated six dimensions critical to ensuring the success of a nation's AI journey. According to the findings, India needs to build upon its investment, data, and strategy in order to accelerate its AI journey. The study also underlines the need for cultural changes and skilling and reskilling workforces to make AI work for the country.

"To succeed in the AI race, India needs to substantially improve its readiness. Leaders should make AI a core part of their strategy and develop a learning agility culture. Investment in this transformative technology has to be continuous for the long-term success. There is an urgent need for talents and tools to develop, deploy and monitor AI models, along with the availability of a robust data estate with the adequate governance," according to Ranganath Sadasiva, Director – Enterprise, IDC.

Building an AI-ready workforce does not necessarily mean an acute need for technological skills alone, notes Srivathsa. "Business leaders will need to drive cultural transformation within their organizations that values experimentation, agility, proactiveness and a growth mindset," she states.

In view of this, a recent Forbes article mentions that while AI is an important opportunity for many businesses, before its integration, business leaders must fully understand AI and the specific subset they wish to use.

Therefore, instead of leaving it to the CIOs or CTOs alone, a CEO must stay informed of AI and the areas of new product development. "Businesses may never meet AI's full capability if it's implemented incorrectly, and probably lose out to competitors who have been focusing on the understanding of the technology. And this does require a strong, collaborative approach," the report says. ■

CIOs Can Embrace A Digital-First Culture To Improve Employee Experience

HR and IT could work better together to improve the digital experience of employees, shows a new study

Companies that provide a positive digital employee experience are more likely to be able to attract and retain top talent, according to a new VMware study that surveyed 6,400 employees, HR professionals, and CIO/IT specialists across 19 countries. Conducted by global research firm Vanson Bourne, the survey finds a startling gap between what IT thinks it is delivering and what employees say they are.

This raises several questions, such as, how much does employee digital experience matter, who in the organization is responsible for digital experience, how well are organizations delivering it, and what can be done to improve it.

Enabling employees with a positive digital

experience entails device choice/flexibility, seamless access to apps, remote work capabilities and an organization's competitive position, revenue growth and employee sentiment.

Digital Experience Gap Exists

The study found that 95% of IT decision maker respondents claim that IT provides employees with the digital tools they need in order to be successful in their job. However, nearly half of employee respondents said they do not have the digital tools they need. And, nearly two-thirds of employees (64%) do not feel they have a voice when it comes to which digital technologies they use at work. In contrast, 83% of CIOs respondents said employees do have a say in this.

Although delivery perceptions differ, both IT and employee respondents do agree on this – digital employee experience projects should be a top priority for their organizations.

The study revealed another gap that employers will want to note – there is a question of who is ultimately responsible for the overall employee experience. IT decision makers most often identified the Chief Information Officer, HR decision makers most often identified the Chief HR Officer, and employees most often identified the Chief Executive Officer.

Despite differences in perception of who is accountable for digital employee experience, nearly all respondents (89%) believe that HR and IT could work better together to improve the digital experience of employees.

Digital Employee Experience Correlates to Key Business Outcomes

Employees' ability to access the apps and information they need, from whatever device or location they choose, affects their ability to effectively plan, collaborate and execute, as shown in the study, affirms the notion that providing employees with a seamless digital experience as they access these resources positively impacts business outcomes including rate of growth, employee sentiment and talent recruitment.

Better Digital Employee Experience Leads to Faster Revenue Growth

80% of employees at companies experiencing high- or hyper-growth (more than 15% revenue growth) report they can easily find and install the right app for any new task/process at work, compared to 42% of employees at companies that are underperforming.

Positive Impact on Workforce Sentiment

Delivering better a digital employee experience also plays a role in workforce sentiment. Respondents who say their organization gives them the ability to work from anywhere as easily as from the office are significantly more likely to say they are proud of their organization, compared to respondents whose company does not enable the freedom to work from anywhere.

The former is more likely to claim their organization has a progressive culture, is recognized as one of the top places to work and provides good work-life balance. In addition, employees are far more likely to recommend their organization (net promoter score) if they work at a company that provides a great digital employee experience.

Job Candidates Consider Digital Employee Experience

Finally, when it comes to attracting new talent, digital experience is something candidates are also noting. A whopping 73% agree that the flexibility of tools (e.g., technology, apps and devices) that they might need to use for work would influence their decision to apply or accept a position at a company.

"Too often, the conversation about digital transformation focuses on the technology and leaves out the key ingredient to a winning strategy – attracting and retaining the best talent. To compete for the best talent, companies are prioritizing employee experience, which encompasses technology, workstyle and culture," says Shankar Iyer, senior vice president and general manager, End User Computing, VMware.

"Leaders committed to improving employee experience are adopting the digital workspace. This fuels modern digital experiences, which our survey revealed as being critically important to current and prospective employees as well as improving other key business outcomes." he adds.

Key Takeaways

From the report, we see a clear lack of understanding from the part of businesses about what employees really want. The need of the hour is a digital-first culture in the organization. But owing to lack of support from senior leadership in the form of funding to concerns over data security when employees use their personal devices to access confidential organizational data – there are several challenges in implementing a digital-first culture in most organizations.

It is then that the CIO or IT specialist has the responsibility to create a robust data security platform to enable a digital culture that HR can evangelize. For example, with the right policies and tools in place, from bring your own device (BYOD) and choose your own device (CYOD) to native app delivery – organizations can strike a balance between employee experience and IT security.

The other interesting finding is that HR alone is not responsible for the digital transformation of an organization. It is here that the CIO, as an enabler of a digital workplace culture can step in to help others adopt the latest technologies. It is the CIO's responsibility to partner with the HR manager, identify the right digital experiences and offer those to their employees.

A collaborative approach would augment work culture, create happy employees and enhance their overall experience. ■

Why CIOs Can't Afford To Ignore Customer Experience?

Many organizations aren't fully committed to providing the level of service they aspire to. As a result, they run the risk of losing customers to competitors, says study

By Sohini Bagchi

The relationship between good customer service and business growth is reciprocal. But a new research shows that many organizations aren't fully committed to providing the level of service they aspire to. As a result, they run the risk of losing customers to competitors.

The 2019 global customer service insights study conducted across the globe by research firm Savanta and commissioned by Pegasystems, surveyed a total of 12,500 customers, businesses executives, and customer-facing employees, reveals that many businesses don't even know their customers well enough to be able to provide the level of service required.

With quality customer service becoming an imperative in the digital era, C-suites are recognizing the importance of delivering a better customer service experience. Despite that brands are failing to create the positive, emotional experiences that drive customer loyalty.

The study poses the question, how willing are key decision makers within organizations to make the transformation required to turn things around? And also with technology at the forefront of every activity in the organization, the CIO (along with other C-suite members) can play a decisive role in boosting customer experience.

The Nuisance of Customer Disconnect

One of the key reasons for poor customer service as shown in the study is that business decision makers are out of touch with their customers, skipping their real pain and problems. No wonder, there exists a huge gap in customer expectations and services offered by brands. 88% of customer-facing employees say that customer service is a priority within their business, but the customers tell a different story.

Their top three frustrations include taking too long to receive service (82%), having to repeat themselves when switching between channels or agents (76%), and not knowing the status of the query (64%). When asked what made for a positive customer service experience, 59% agree that a quick resolution of their issue or question mattered most, followed by a need for knowledgeable service agents (48%) and a fast response (47%). The study researchers say, this can provide businesses with a clear roadmap for improvement.

Poor Service can Cost Businesses 'Customers'

Three-fourths of customers surveyed in the research agree that the standard of customer service they receive is a major determining factor in their brand loyalty. In addition, nine out of

CIO can create strategies around technology or build tools and technology systems

10 say receiving poor customer service from a business damages their impression of the brand.

A whopping 75% also say they have previously stopped doing business with an organization because of poor customer service. Nearly half the customers in the report say that if they receive a negative customer service experience, they immediately stop the purchase and move to another vendor.

A point to note is that 35% of business decision makers say they lose customers 'all the time' or 'fairly regularly' as a result of providing poor customer service, as per the study and they are not doing much about it, costing businesses millions of dollars.

Another research, NewVoiceMedia's 2018 'Serial Switchers' report reveals that poor customer service is costing businesses more than USD 75 billion a year. The report claims, as customers do not feel appreciated or are misbehaved or harassed in some way by the staff or because of technical glitches, 67% customers have become "serial switchers," customers who are willing to switch brands because of a poor customer experience.

"Good customer service can be the difference between success and failure, and what this study tells us is that organizations still have a long way to go before they are able to meet the expectations of their customers," Suman Reddy, Managing Director, Pegasystems India states.

Why CIO Should Step In

While the study aims at the key decision makers in the organizations urging them to rethink on successful customer service, CIOs have a key role in enhancing the quality of customer service in the digital age.

CIOs have a dynamic role in today's tech-driven enterprises. Whereas they were once solely focused on technology infrastructure, the data-driven and technological nature of today's business world is pushing the CIO into the limelight.

As far as the CIO's role is concerned, instead of simply focusing on internal stakeholders, they are now paying attention to the business side of tech, thereby creating a more meaningful user experience, both internal and external. They therefore have a say in the customer experience conversation.

As technology becomes a more crucial component for driving the overall CIO can create strategies around technology or build tools and technology systems that are designed to improve customer success. As Reddy believes that technology solutions are available to help businesses understand and proactively address customer issues, while also arming customer-facing staff with the tools they need to provide more contextual, relevant, and knowledgeable service.

A close collaboration between CIO and the C-suite, (IT and business is becoming more important than ever to create a win-win situation for business and customers that can have a positive impact on the bottomline. ■

As Multi-Cloud Becomes Mainstream, Here Is What You Can Do

The need of the hour is a multi-cloud management strategy that will help CIOs understand and overcome the primary obstacles

By Sohini Bagchi

Multi-cloud has been there for a while, but challenges of interoperability and complexities have often dissuaded enterprises from large-scale adoption. Times are now changing, as enterprise awareness of the cloud has increased and organizations across the globe are moving forward with digital transformation initiatives. Consequently, CIOs opt to work in a broader-based, more diverse IT landscape founded on a multi-cloud environment.

According to an IDC report, more than 70% of companies are using multiple cloud environments today. In that CIOs continue to deal with issues related to security and governance policies, the need for optimization of resources and cloud consumption costs, as well as the need for automation of business applications and data workflows. This often stifles innovation and adds complexity.

Nonetheless, when effectively implemented, CIOs can reap immense benefits from multi-cloud environment. As Daphne Chung, Research Director for Cloud Services and Software at IDC Asia/Pacific observes, "With organizations gravitating towards a multi-cloud environment, they will find themselves increasingly dealing with the growing complexity, ensure integration and portability of workloads as they seek to achieve greater levels of innovation and business value."

The need of the hour is a multi-cloud management strategy that will help CIOs understand and overcome the primary obstacles in order to realize the success in a multi-cloud environment. Here are a few ways to ensure CIOs can establish a successful multi-cloud strategy for improved performance, total cost savings and rapidly respond to business requests.

1. Select Cloud Partners Smartly

"Each cloud service provider fits your specific needs and budget. However, since you are also going to be working with multiple cloud partners, you should ensure that the cloud platforms and tools are compatible and are not redundant," states Gangadhar S J, Head – Technology at Digit Insurance.

"You can mix and match the best combination, so that the enterprise is not restricted to one cloud provider for all its data storage needs. CIOs can chalk out the features from each cloud service provider and how each worked with the others," adds Gangadhar.

For example, Amazon's AWS rides high on its cost-effectiveness; Microsoft Azure offers a robust enterprise presence, while Google's GCP is best in the field of analytics. With multi-cloud

in place, an enterprise can benefit immensely from all of these factors, so that you can choose the cloud platform which best suits your needs.

There are also chances that your cloud providers are not fully compatible in terms of the setup and configuration of underlying infrastructure components for both the networking and security components. Therefore, when looking at a multi-cloud strategy, CIOs should have the detail on how scalability and security will be initially set up and maintained.

2. Keep an Eye on the Costs and Accounting

The CIO must keep a close watch on the costs and accounting for the expenditure across all the tools and providers. This can be a daunting task, but a very effective way to do this is to use a mapping strategy. It is important to monitor how much time the IT team spends using, managing and troubleshooting it, how that cloud tool reduces other costs and the overall benefit it provides.

"CIOs using various cloud services, should aim at optimizing IT costs based on specific workloads or projects, such as finding the cheapest way to deal with test and development requirements for a project that may only run for a short period of time," Makarand Sawant, Senior General Manager – IT, Deepak Fertilisers & Petrochemicals Corp says.

3. Think Beyond Just Multi-cloud

For multi-cloud management process, CIOs should consider the overall cloud management system in use and how the organizations need to continually evolve along with emerging technology and new cloud options. In other words, what matters is, how efficient it will be to integrate the existing and potential cloud technology, as well as how productive the overall system can make the organization as it becomes embedded in processes and departments.

"When looking to manage a multi-cloud environment, it is important to understand these complexities, and how to avoid costly mistakes. To avoid supplier lock-in, businesses are looking at a multi-cloud strategy, where they take their pick from the best cloud applications, platforms and infrastructure offerings to work alongside in-house systems in their datacenters," Sawant says.

"The benefits of deploying multiple cloud services go well beyond matching application requirements. They enable us to fine tune our capabilities to meet or exceed our business requirements, and focus on what matters most to the business," he adds.

Multi-cloud is becoming the de facto standard as its adoption has grown manifold in enterprise

4. Re-evaluate on a Regular Basis

Any successful multi-cloud strategy must detail how the current strategy should be re-evaluated to ensure it continues to meet business demands. Every component of multi-cloud should be formally audited at set time intervals throughout the year.

"Rigorous evaluation of multi-cloud is essential as it helps IT teams identify new opportunities with cloud providers and help address security concerns, data protection and protocols, availability and the cloud management," Antonio Vargas, Principal Product Manager for BMC, says in his blog.

For instance, some decisions that were correct from a business strategy even six months ago may have dramatically changed today. Hence, it's necessary to re-evaluate your strategy at least once every year.

5. Multi-cloud is About the Entire Organization; Not Just IT

Although it may appear that multi-cloud management is the sole responsibility of IT, it's really about the entire organization and involves functions across your enterprise. CIOs should involve the entire executive team and explain to them what each cloud tool and platform does. He should explain to them what impact multi-cloud can have on individual and overall performance.

"Aligning everything within the multi-cloud management process with the company's strategic objectives and quantitative results can help everyone understand the context for investing in the cloud and the value of its adoption," says Subram Natarajan, CTO, IBM India South Asia.

6. Have a Multi-cloud Management Structure

While it is important for the CIO to share responsibility of multi-cloud practices, he/she should put in place a strong structure for cloud management. This includes creating a team within IT to help the CIO rigorously assess cloud vendors and tools on the basis of their relevance and performance.

The CIO and IT team should gear up to think more about how the cloud works, what's possible and what still needs improvement. We are gradually moving towards a multi-cloud world – a phenomenon described in RightScale's *2019 State of the Cloud Report* (now part of Flexera), which states that multi-cloud is becoming the de facto standard, as its adoption has grown manifold in the enterprise.

A multi-cloud environment is complicated, time-consuming and testing, at times. However, it also brings a new level of efficiency, cost containment and productivity that never existed prior to implementing multiple cloud platforms and tools. Experts believe, it is a process that will evolve over time with new technology and changing organizational objectives. ■

Can CISOs Step In To Solve The Impending Cyber-Security Crisis?

New research indicates that CISOs need to work in close coordination with other C-suite members

Cyber-security skills shortage is putting businesses at risk in a variety of ways, according to a new study, which suggests that most organizations are struggling to address the cyber-security skills shortage, and consequently the effects of the shortage are worsening. The study further focuses on the Chief Information Security Officers (CISOs) suggesting ways they can step in to solve the looming cyber-security crisis.

In its third year, the study conducted by the Information Systems Security Association (ISSA) and analyst firm, Enterprise Strategy Group (ESG) surveyed 267 cyber-security professionals

worldwide, including India. The cyber-security skills shortage is now affecting 74% of organizations, according to the report, yet 63% of organizations are falling behind when it comes to providing adequate levels of training to their cyber-security staff, it says.

The report further confirms that the cyber-security skills shortage continues to be the root cause of rising security incidents, as organizations remain plagued by a lack of end-user cyber-security awareness and the inability to keep up with the growing cyber-security workload. Almost half (48%) of respondents have experienced at least one security incident over the past two years with serious ramifications including lost productivity, significant resources for remediation, disruption of business processes and systems, and breaches of confidential data.

CISOs, for example, are downright skeptical about their chances for success. 91% believe that most organizations are vulnerable to a significant cyber-attack. And an overwhelming 94% believe that the balance of power is with cyber-adversaries over cyber-defenders. No wonder then that organizations are facing increasing and potentially devastating cyber-risks.

Areas of Acute Skills Shortage

The most acute skills shortages shifted this year to cloud security (33%), followed by application security (32%) and security analysis and investigations (30%), according to the study.

"In an era where business leaders are more reliant on technology for success and are facing more scrutiny and accountability than ever before, this lack of progress and the resulting cyber-risk for organizations and their shareholders, customers and business partners should be a cause for concern for business and technology leaders alike," the report says.

The research also indicates an alarming personal impact related to cyber-security jobs. While CISOs remain dedicated to their craft, attracted by the deep technical challenges and moral implications, the study explores the causes and consequences of stress and burnout.

- **Stressful aspects of the job:** 40% responded with keeping up with security needs of new IT initiatives, followed closely by "shadow" IT initiatives, trying to get end-users to better understand cyber-risks and change their behavior, and trying to get the business to better understand cyber risks.
- **Added stress of new data privacy responsibilities:** Even though regulations, such as GDPR is in full swing, cyber-security teams may not be up to the task. 84% claim that the cyber-security team at their organization has taken a more active role with data privacy over the past 12 months, but 21% don't believe the cyber-security team has been given clear directions and 23% state that the cyber-security team has not been given the right level of training.
- **Job-related pressures driving virtual CISO (vCISO) as attractive career option:** One out of 10 organizations now hires a vCISO. At present, 29% of CISOs interviewed in the survey are working as a vCISO while 33% would consider it in the future. Almost half claim that working as a vCISO brings more variety and flexibility to a CISO position. Also, CISOs are clearly seeking to avoid some of the politics and stress while taking more control of their careers.

Based upon the results of this report, one can conclude that cyber-security progress has been marginal at best over the last three years. As Jon Oltsik, Senior Principal Analyst and Fellow at the Enterprise Strategy Group (ESG) and the author of the report, notes, "We may be making some cyber-security improvements but we are getting worse faster. This issue should be of concern to technologists, business executives and private citizens and continues to cause an existential threat to national security."

Candy Alexander, CISSP CISM, Executive Cyber-security Consultant and ISSA International President, adds that the problem today is that organizations are looking at the cyber-security skills crisis in the wrong way; it is a business, not a technical, issue.

"Business executives need to acknowledge that they have a key role to play in addressing this problem by investing in their people. Also, business leaders need to get involved by building a culture of support for security and value the function," comments Alexander.

Lessons for the CISOs/Security Experts

- CISOs need to be more active with business executives. They should seek a seat at the board table and work in close coordination with other C-suite members. For example, he/she should work in close coordination with HRO to come up with training program and coordinate with CIO to cast a wider net beyond IT and find transferable business skills and cross career transitions will help expand the pool of talent.
- Enhancing soft skills could be a turning point to a CISOs career. CISO's success depends upon characteristics like communication skills, leadership skills, a strong relationship with business executives, and a strong relationship with the CIO and IT leadership team.
- For CISOs and security teams to stay afloat they must constantly nurture their skill sets/domain knowledge. Security certifications such as CISSP are becoming essential.
- Experts also suggest security professionals to prioritize practical skills development over certifications. Attending specific cyber-security training courses, participating in professional organizations and events, attending trade shows, and participating in on-the-job mentoring programs can make a difference in the way CISO and his team deals with cyber-security. ■

IoT Security Breaches Drive CIOs To Lead From Front

Most boards don't understand the importance of IoT risk exposure and the CIO has a role to play here

Unsecured Internet of Things or IoT devices in the workplace and those used by third parties are causing large scale cyber attacks, disrupting the privacy and security of organizations. But most boards don't understand the importance of IoT risk exposure. While on one hand, this is giving a more challenging time to CIO/CISOs, it also offers them a great opportunity to take a leadership position on IoT.

Researchers have identified a significant uptick in breaches and attacks related to IoT in a new Ponemon Institute report. It further states that most companies don't know the depth and breadth of the risk exposures they face when leveraging IoT devices and other emerging technologies.

Released by the Santa Fe Group, the study yielded 35 key findings on IoT risks stemming from a lack of security in IoT devices. Ponemon Institute identified a sizable increase in the number of organizations reporting an IoT-related data breach. In 2017, only 15% of survey participants had suffered an IoT-related data breach. That number jumped to 26% in this year's report, which surveyed over 600 CIOs, CISOs, chief risk officers in the US and other regions including India.

"The actual number may be greater as most organizations are not aware of every unsecure IoT device or application in their environment or from third party vendors," the report said. In fact, the study found that more IoT security issues are being reported at the third-party level.

Over the last year, 23% of respondents said they experienced a cyberattack and 18% said they had a data breach caused by unsecured IoT devices among third-party vendors. Even those who have yet to identify a breach feel certain that the future of IoT will be weighed down by risk.

More alarmingly, organizations surveyed have no centralized accountability to address or manage IoT risks. Less than half of company board members approve programs intended to reduce third party risk and only 21% of board members are highly engaged in security practices and understand third party and cyber security risks in general. More than 80% of respondents believe their data will be breached in the next 24 months.

The current findings are equally gloomy, as the study found that only 9% of respondents said their companies have education policies to inform employees about IoT third-party risks and nearly a third (32%) do not have a designated person in their department or organizations who is responsible for managing IoT risks.

"Board members of organizations need to pay close attention to the issue of risk when it comes to securing a new generation of IoT devices that have found their way into your network, workplace and supply chain," said Cathy Allen, founder and CEO of The Santa Fe Group, Santa Fe, NM. "The study shows that there's a gap between proactive and reactive risk management. The time to address this issue is now and not later."

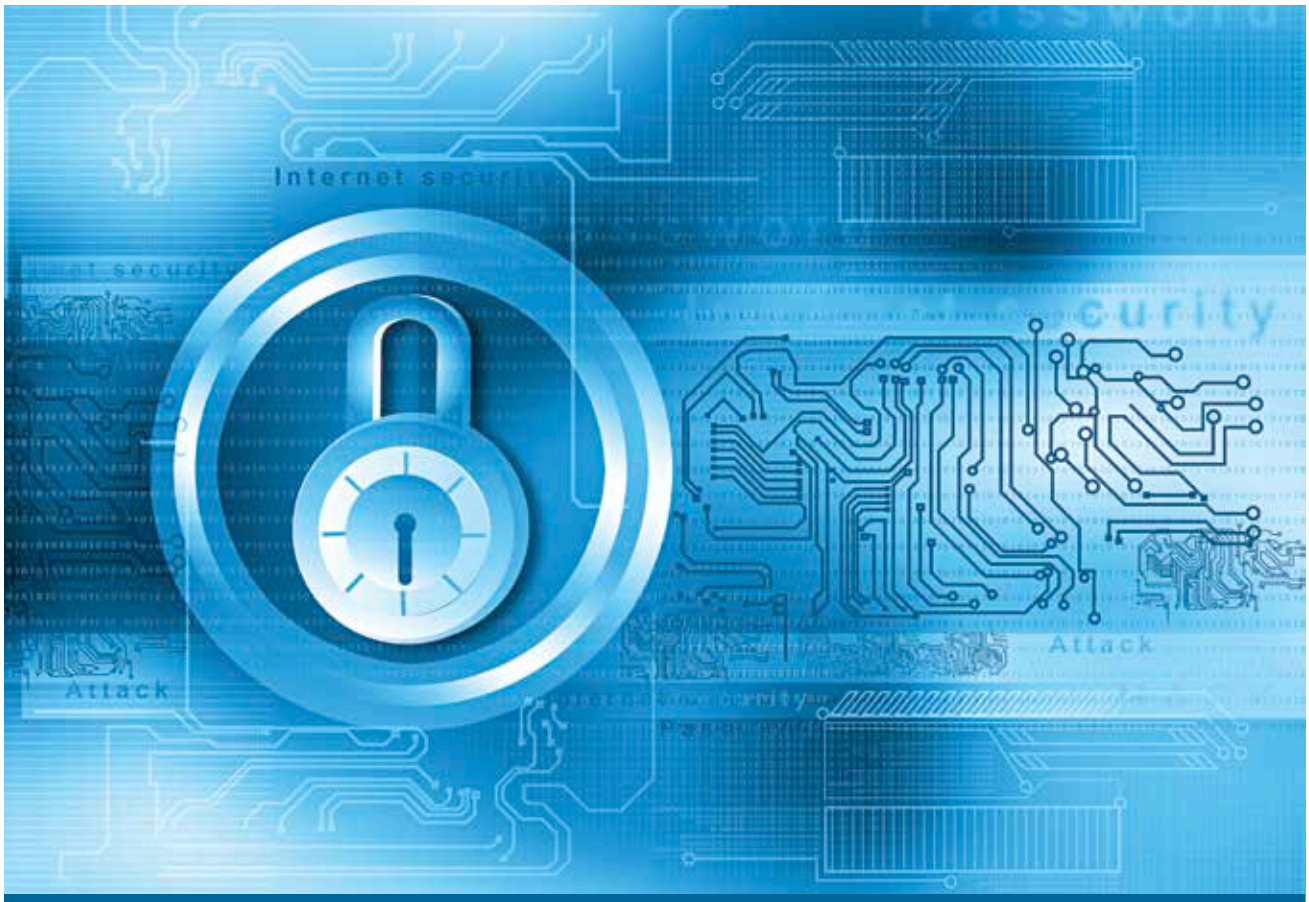
What CIO/CISOs Can Do?

From the Ponemon report, one thing is clear that IoT is increasingly affecting the enterprise in a very big way, and there's a role for CIOs, and CISOs.

However, it may not be based on the way traditional organizations want to govern the risk. In view of that CIO/CISOs might get more into the business function than compliance or risk management function. Here are some recommendations:

- Ensure inclusion of third-party and IoT risks occurs at all governance levels, including the board.
- Update asset management processes and inventory systems to include IoT devices, and understand the security characteristics of all the inventoried devices; if devices have inadequate security controls, replace them.
- Review contracts and policies for IoT-specific requirements and update them to include such requirements if necessary.
- Expand third-party assessment techniques and processes to include controls specific to IoT devices.
- Develop specific sourcing and procurement requirements around security of IoT devices.
- Devise new strategies and technologies for reducing threats posed by IoT devices.
- Collaborate with experts, peers, associations and regulators to develop, communicate and implement best practices for IoT risk management.
- Include IoT in communication, awareness and training at all levels, including the board, executive, corporate, business unit and third parties.
- Recognize that your organization is increasingly dependent on technology to support the business and the risk posed by this dependence.
- Embrace new technologies and innovations, but ensure security controls are included as fundamental and core requirements.

In conclusion, CIO/CISOs can drive organizations to better understand the inherent risks posed by IoT devices in their supply chain, ensure IoT security is taken seriously, and influence the board in educating management at all levels — including governing boards. They should also ensure that IoT security concerns are integrated into the device design/build phases of product development. ■



Threat Intelligence Can Help CISOs Mitigate Security Risks, Says Study

Here are the key findings and takeaways for CIO/CISOs from the recent Fortinet Threat Landscape Q1'19 report

In recent years, cyber security attacks have increased substantially and companies have to bear phenomenal losses to safeguard themselves from the clutches of security threats. The latest threat landscape report from Fortinet for Q1 2019 shows that cyber criminals are not just becoming increasingly sophisticated in terms of their attack methods and tools, they are also becoming very diverse, throwing greater challenges to IT and security professionals.

The Fortinet report explains how attackers are increasingly using a broad range of attack strategies, from targeted ransomware to custom coding, to living-off-the-land or sharing infrastructure to maximize their opportunities, and using pre-installed tools to move laterally and stealthily across a network before instigating an attack. Based on the report findings, we provide

insight into how CIO/CISOs should adopt a proactive approach, such as threat intelligence and other techniques to curb cyber security risks.

Here are some of the highlights of the research:

- **Majority of threats share infrastructure:** The degree to which different threats share infrastructure shows some valuable trends. Some threats leverage community-use infrastructure to a greater degree than unique or dedicated infrastructure. Nearly 60% of threats shared at least one domain indicating the majority of botnets leverage established infrastructure. This makes it clear that infrastructure plays a particular role when used for malicious campaigns. Understanding what threats share infrastructure and at what points of the attack chain enables organizations to predict potential evolutionary points for malware or botnets in the future.
- **Ransomware far from gone:** In general, previous high rates of ransomware have been replaced with more targeted attacks, but ransomware is far from gone. Instead, multiple attacks demonstrate it is being customized for high-value targets and to give the attacker privileged access to the network. Some of the recent ransomware variants such as LockerGoga demonstrates that CISOs need to remain focused on patching and backups against commodity ransomware, but targeted threats require more tailored defenses to protect against their unique attack methods.
- **Pre- and post-compromise traffic:** The Fortinet research demonstrates if cyber criminals carry out phases of their attacks on different days of the week. It finds out when comparing Web filtering volume for two cyber kill chain phases during weekdays and weekends, pre-compromise activity is roughly three times more likely to occur during the work week, while post-compromise traffic shows less differentiation in that regard.
- **Content management needs constant management:** New technologies such as Web platforms are getting a lot of attention from cyber criminals recently. These platforms make it easier for consumers and businesses to build Web presences. They continue to be targeted, even associated third party plugins, says the study.
- **Tools and tricks for living off the land:** Threat actors increasingly leverage dual-use tools or tools that are already pre-installed on targeted systems to carry out cyber attacks. This "living off the land" (LoTL) tactic allows hackers to hide their activities in legitimate processes and makes it harder for defenders to detect them. These tools also make attack attribution much harder.

Michael Joseph, Regional Director System Engineering, India & SAARC, Fortinet believes that CISOs need to rethink their strategy to better future proof and manage cyber risks. He suggests, "Embracing a fabric approach to security, micro and macro segmentation, and leveraging machine learning and automation as the building blocks of AI, can provide tremendous opportunity to force our adversaries back to square one."

While the malicious attempts to damage systems of a firm are increasing, they are also getting more complex. To stay ahead of cyber threats, CIO/CISOs must evaluate their cybersecurity processes to make sure that effective systems are in place.

Here are some of the key takeaways for CIO/CISOs:

1. Invest in threat intelligence programs

In order to understand existing or potential hazards targeting valuable assets, firms rely on threat intelligence. The information gathered is used to identify, prevent and react to such threats through informed decisions. With threat intelligence program, CIO/CISOs can stay up to date with security threats, including methods, targets and vulnerabilities. Fortinet researchers recommend only a security fabric that is broad, integrated, and automated can provide protection for the entire networked environment, from IoT to the edge, network core and to multi-clouds at speed and scale.

2. Combine IT security and business risk management

As cybersecurity is not just an IT-related threat, its impact could even have greater legal and regulatory implications. That is why IT security needs to blend with business risk management strategy too. CIO/CISOs need to support IT governance, including data security, as a way to ensure IT strategy aligns and supports the business' overall objectives.

3. Ensure smooth C-suite communication

The lack of collaboration at the C-suite level is creating cybersecurity risks in the enterprise. A report by Accenture states that only 40% of CISOs surveyed said that they always communicate with other business managers proposing an integrated security approach.

4. Create a ransomware defense

Detecting and preventing ransomware has become imperative. Hence CISOs need to understand the nature of ransomware attacks and what they are targeting—geography and vulnerabilities. They should prioritize patching and establish backup, storage, and recovery activities.

5. Be careful of pre-installed tools

Organizations must pay particular attention to pre-installed tools that can be exploited to escalate privilege and hide malicious code and attacks. Intent-based segmentation uses business logic to segment the network, devices, users, and apps, can prevent lateral movement of LoTL attacks, thereby, preventing them from accessing critical data and infrastructure.■

Protect Your Business – 6 Reasons Why Data Backups Are Important

Having proactive data backup procedures in place allows you to handle any unforeseen data loss situations, keeping your productivity and brand stable

By Giridhara Raam M

The increase in ransomware attacks and high-profile data breaches over the last few years has reinforced the importance of data security. Recent research indicates that an average of 2,244 cyberattacks happens globally each day, and many of these attacks are targeting sensitive business data. Large enterprises are clear treasure troves of data in the eyes of hackers, but small and medium-sized businesses (SMBs) are often targeted as well. Businesses are becoming more dependent on data in the 21st century, which means the demand for data security is increasing.

However, data security isn't just about protecting data from malicious outsiders; remediation is a critical aspect of data security. While you can't predict when data loss will happen, you can make sure your business has the right solutions to recover its critical data. IT managers are responsible for implementing the right data backup and disaster recovery procedures in their businesses.

Mentioned below are a few reasons why your business needs to perform data backups and implement a disaster recovery solution:

1. Preventive measures don't always work

Businesses should take a proactive approach to cybersecurity by equipping themselves with network security solutions, strong firewall configurations, and patch management tools, but they also need solutions for mitigating data loss. SMBs are clearly not immune to having their data stolen or encrypted by ransomware, but according to research by Nationwide Insurance, 68% of SMBs don't have a disaster recovery plan. Every organization, big or small, needs to have a plan for mitigating the aftermath of natural disasters, server downtime, and other complex situations.

2. Cyberattacks are constantly evolving

According to a CNN report, the average small business hit with ransomware in 2017 lost over USD 100,000 due to downtime. What's more, these businesses struggled to recover their encrypted data, if they were able to recover it at all. Ransomware is just the tip of the iceberg in terms of cyberattacks; malware, DDoS attacks, data breaches, supply chain attacks, and zero-day exploits are a constant threat.

These cyberattacks usually target sensitive business information stored in the cloud or on-premises. The fre-

quency of cyberattacks has increased thanks to digital transformation, which has become a key driver for businesses in every industry. Businesses today are seeing a massive influx of data for every activity from lead generation to customer conversion, and attackers are ready to capitalize on this steady stream of data.

3. Natural disasters can halt business in an instant

According to Clutch, 60% of small businesses that lose their data will shut down within six months. Although data can be lost in many ways, you should never underestimate the occurrence of catastrophic natural disasters. Regardless of your business' size, you need to prepare for storms, earthquakes, fires, and any other natural disaster that could shut down your servers and datacenters.

4. Lost data hurts your brand's reputation

According to a study by Small Business Trends, 58% of businesses don't have a backup plan for data loss. What businesses need to consider is that, in addition to the above points, data loss leads to a loss of customer trust. Being known as a company that has lost data, especially customer information, won't do your business any favors. In fact, having a poor reputation will likely lose you customers and may impact your organization's productivity since new employees might hesitate to join your company.

5. Cloud computing demands additional backups

Moving your on-premises operations to the cloud can save your business money and reduce its management efforts, but the cloud isn't without its risks. When businesses store their corporate data on the cloud, they're placing the security of that data into the hands of the cloud provider.

6. Insider threats are often unseen

You never know whether one of your employees will pose a threat to your business' data. A disgruntled employee could easily steal or erase business-critical data if you don't have proper security controls in place. According to a survey by CA Technologies, 56% of cybersecurity professionals say regular employees pose the biggest security threat to organizations, with excessive access privileges being the main enabler of insider attacks.

Having proactive data backup procedures in place can add additional security for your business. It also allows you to handle any unforeseen data loss situations, keeping your productivity and brand stable. Since data loss can happen at any time and in a multitude of ways, just making backups is a good place to start. However, keeping consistent backups is the key. If a disaster strikes and your last backup is six months old, your business will have a hard time recovering. Likewise, your data backup plan should be coupled with a disaster recovery plan. This will give you an extra hand when you need to restore your failed devices as quickly as possible. Your corporate data management procedures should include software that automatically creates backups and makes restoring from different backup versions as easy as possible.

Additionally, the 3-2-1 rule is often recommended for maintaining backups: Keep three total copies of your data, in two different mediums, with one copy stored off-site. Maintaining physical backups even if you use cloud storage is advised in case your cloud provider experiences downtime or faces a breach.

Best practices for data security

When it comes to databases in particular, here are a few security best practices that could help your business fight against database takedowns and breaches:

1. Define strong password policies.
2. Remove stale user accounts.
3. Change the default username for admins.
4. Restrict user privileges.
5. Encrypt sensitive business data.
6. Keep applications and firmware up-to-date.

Special note should be placed on that last point. According to Gartner's predictions, 99% of vulnerabilities exploited by 2020 will continue to be the ones that security and IT professionals have known about for at least one year. This extends beyond just databases and is something to keep in mind for all data storage operations.

Lastly, you need to audit employee login and logoff behavior, manage USB connections, and provide employees with only the minimal amount of privileges needed for them to complete their work. You don't want to have an air-tight storage and recovery plan unraveled by a malicious insider or an irreversible mistake. ■

The author is Marketing Analyst at ManageEngine

Double Scoop

Two times the revelation

Vijay Pukale

Program Manager
Tieto

MY FAVORITE SPORT

Cricket

A TECH EVENT I ATTENDED RECENTLY

'Project Management Forum' organized by Tieto in April 2019

A TECH AREA I LOVE THE MOST

Cloud Computing

MY FAVORITE POLITICIAN

Narendra Modi

A PLACE WHICH I WOULD LIKE TO VISIT MORE OFTEN

Matheran (near Pune)

MY PEER IN THE IT COMMUNITY

Sandeep Kumar Upadhyay,
DGM, Vodafone Idea

Sandeep Kumar Upadhyay

DGM, Vodafone Idea

MY FAVORITE ACTOR

Kishore Kumar

MY FAVORITE SINGER

Kishore Kumar

AN EMERGING TECH THAT I WOULD LIKE TO WORK ON

IoT

A GADGET I USE FREQUENTLY

Smartwatch

MY FAVORITE DRESS

Semi-formal

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।

digit.in
NOW IN HINDI

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

डिजिट

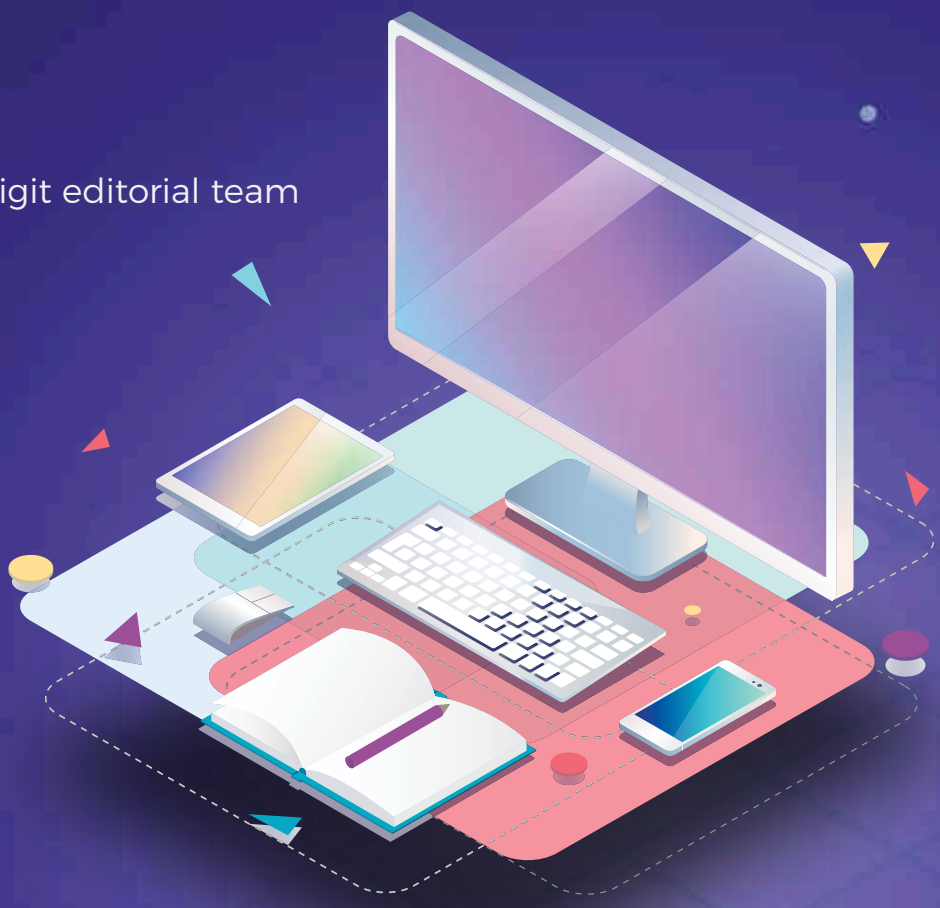
LAUNCHING

digit SQUAD

Here is your chance to become a Digit certified tech influencer

Benefits of Digit Squad Member

- Launch your own tech channel on Digit.in
- Become a Digit Certified tech influencer
- Engage with digit editorial team
- Make money



Apply now by scanning the QR code

www.digit.in/digit-squad/apply.html

PAHWA™ GROUP
Innovation is life

Replacement Service for any make of Chemical Filter

Bry-Air

We replace spent media immediately with
UL Certified Granular and Honeycomb Chemical Media

Bry-Air®
BRYSORB™
Granular Media

Bry-Air®
DRISORB™
Honeycomb
Chemical Filters

Contact today!

Backed by
Brycare™ Service

BRY-AIR (ASIA) PVT. LTD.
www.bryair.com
Phone: +91-124-4184444 • E-mail: bryairmarketing@pahwa.com
Plants: India • Malaysia • China • Switzerland • Brazil • Nigeria
Overseas Offices: Vietnam • Indonesia • Philippines • Korea • Japan • UAE • Saudi Arabia • Bangladesh • USA • Canada

Leaders in Gas Phase Filtration Systems

RB/BA/1923FCA3