Data Center | Pg 14
What Exactly Is A Data Center Park?

Insight | Pg 16
Disruptive Changes & Regulatory Pragmatism

ITNEXT

FOR THE NEXT GENERATION OF CIOs

INDIA's FUTURE CIOs

NEXT100 2019 AWARDS

Presenting to you a glimpse of the NEXT100 2019 Awards, held at New Delhi, Mumbai and Bengaluru...

February 2020 | ₹100 | Volume 10 | Issue 08 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

PA WA GROUP
Innovation is life

Process Industries

TRANSFORM A CORROSIVE WORK ENVIRONMENT INTO A SAFE ONE

Bry-Air®

Turnkey Services

Detect, monitor, and remove corrosive air-borne pollutants from electronics-intense work environments, so also check the residual life of chemical media and replace it.

Call today. Prevent breakdowns.

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

RB/BA/1921FCA3

Leaders in Gas Phase Filtration Systems

The myths around enterprise IT decision making

If the CIOs get into the product specifications to decide each point solution, just imagine what will happen to the big transformation we all keep talking about!

Shyamanuja Das

We just hosted our NEXT100 award ceremony this year—a little later than the normal time we do it, in November-December.

Without any pretension, let me tell you the reason. It is lack of sponsor interest in the event that forced the delay. If we still decided to host it, it is because it is our commitment to the community.

NEXT100 is done primarily for the community, with active participation from the senior-most members of the community as jury members and as supervisors who encourage their juniors to participate. So, despite all odds, we decided to do it, without taking out any of the essential components of the recognition—the trophies, the certificates, the NEXT100 book, the NEXT100 club badges and so on; of course, with some austerity in the event arrangements. In hindsight though, jury members and awardees liked the interaction opportunity that this format gave them.

But let me come to the point. Do you know what was the reason behind sponsors shying away? They think they needed to reach out to only CIOs. Many of them organize their own events—often in association with us—and try to invite CIOs and present them technical details of the product. CIOs have been telling us—and now they tell that in open—that evaluation of tech features of a solution is something not done by them at all, but by the next level managers—the best of whom are recognized by NEXT100 awards, every year, for the last 10 years. A few jury members—senior CIOs—did repeat that observation in the award ceremonies.

It would have been a different matter if the technology vendors would have reached out to them through some other means, and not through us. As an editor, I would not have probably noticed that.

But if they say they do not want to reach out to these people because they think it is the CIOs who decide on each and every feature of an IT solution, it is difficult to ignore.

It is a huge understanding gap.

That gap does impact the sales cycle; and in turn, the technology investment and rollout plans in the enterprises. If the CIOs—who are now expected to show the CEOs the new technology-leveraged business possibilities—get into the product specifications to decide each point solution, just imagine what will happen to the big transformation we all keep talking about!

That is my concern.

As CIOs get ready to meet this new expectations, they are delegating the product evaluation level decisions to the next level managers. Most of them have already done that.

It is just the myth that needs to be busted. ■

FEBRUARY 2020
VOLUME 10 | ISSUE 08

Content

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: Baiju NV
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
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

Back to nature: An annual holiday that takes one close to the nature is reinvigorating

Enjoy Being By Yourself

NEXT100 Winner 2016 **Meetali Sharma,** Corporate Risk, Compliance & Information Security Leader, SDG Software India shares her love for the beauty of nature and how it helps her escape from the rigors of urban life

"Nature always wears the colors of the spirit."
– Ralph Waldo Emerson

"Holidays – any holiday – are such a great opportunity to focus on bringing the family together."
– Lidia Bastianich

Every year we go on a family holiday where we are completely away from social media and unnecessary phone calls. "Hartola", a small village in Uttarakhand, is where we have built a small holiday home and it is our escape from the urban world.

Our holiday generally lasts from 7-10 days. A typical day at Hartola begins with "Himalayan glacier view" from the window followed by nature walk around the village. We make sure to plant 3-4 saplings each day during our stay. Afternoons are filled with outings, outdoor games, camping, painting with natural colors, reading books, plucking fresh fruits and enjoying soft music. We enjoy our evenings with barbeque using fresh farm grown local organic vegetables.

Apart from all this, we also make sure to meet the villagers and help them in whatever way we can which may be giving some food items, distributing clothes or helping them with some paperwork. We also visit the nearby schools and distribute stationary and sweets to students and encourage them to continue their studies. Overall, the experience is always enriching. ■

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.

Dance is a passion that keeps the love blossoming, mind cool and faculties sharp. The rhythms of dance help ace the rigors of life

Feeling The Rhythmic Movement

NEXT100 Winner 2018 **Ankit Aggarwal,** Head - IT, PI Industries (Udaipur) shares his immense passion for dancing and how it has transformed both his personal and professional life...

"Hand in hand, on the edge of the sand, they danced by the light of the Moon." ***– Edward Lear***
"Dance is the hidden language of the soul." ***– Martha Graham***

Since childhood I was fascinated by the adage 'Jack of all trades'. I spent three decades of my life being a 'Jack'. I love music, dance, writing poetry, art and craft, extempore, photography and many other creative activities. But as I began getting more involved in my professional life, some of these activities took a backseat. Only two things can revive a passion – love and parenthood – and that is exactly what I have experienced.

My wife and I have never missed an opportunity to dance to the tunes of our love, whether it is at a sibling's wedding, a DJ playing loud music in a party or a secluded palace on a lakeside. Our love for each other blossoms and becomes a catalyst for our love for many months to come.

Often, we've hired choreographers to train us for a formal performance and ended up forgetting the steps on the final day. But the coordination and trust between us helped us dance away. We create such comfort zones for each other that we don't miss a beat. Dance helps strengthen partnership, adaptability and trust between us and we forget the world around us when are dancing. Despite my plus-size built, my passion for dance does not let me tire and whenever there is an opportunity, there is a dance for me. I'm fearless, creative and collaborative when I dance and this helps me a lot in keeping a cool mind both at home and at workplace. This passion for dance has begun building in my daughter and when we stand in front of the television in the morning, we dance to the music..

For me, life without music and dance is like my work: IT without a computer. This love has helped me several times at work too. I can easily gel or collaborate with people, work in sync and harmony, adapt to any challenges and changes easily and be always on my toes. Dancing helps me to keep stress miles away and helps to rejuvenate me after a hard day at work.

I feel if I spend some more time on my passion, I would also be able to derive health benefits through it. I must dedicate more time to dancing and I am sure I would cultivate my passion even more than ever. ■

As told to Dipanjan Mitra, Team ITNEXT

Ankit Aggarwal

Snapshot

Ankit Aggarwal is Head - IT at PI Industries (Udaipur). He is NEXT100 Winner 2018. Earlier, he was associated with E.I. DuPont India and Satyam Computer Services. He has an MBA in International Business from Indian Institute of Foreign Trade and BTech in Electronics & Communication Engineering from Dehradun Institute of Technology.

INDIA's FUTURE CIOs

NEXT100 2019 AWARDS

Presenting to you a glimpse of the NEXT100 2019 Awards, held at New Delhi, Mumbai and Bengaluru...

Welcoming the Tenth Batch of NEXT100

The 2019 winners of NEXT100—the 10th batch of this community awards—were formally welcomed to this exclusive club in three separate award ceremonies held in New Delhi, Mumbai and Bengaluru between 27th to 29th February 2020.

This is the first time the awards were held in three locations, closer to where winners actually are.

The format was also significantly different. The grandeur and formality were replaced by insightful and practical advice to the award winners by jury members of NEXT100—all eminent CIOs from the industry—followed by engaging discussions between the two sets—one representing experience and the other energy & ideas.

With 2019 winners, the NEXT100 club is now 1000 members-strong. In all these years, the process of selection has seen 25,000+ registrations, 3000+ interviews by 200+ Jury members, and of course, 1000 winners from more than 40 locations across India.

The award ceremony, started in 2010 in Ramoji Film City, Hyderabad, has now been held in seven cities—Hyderabad, Pune, Gurgaon, New Delhi, Amritsar, Mumbai and Bengaluru, with Pune hosting it a record four times.

This year's three-city format—though it denied the awardees in different cities to meet with each other in person (something that they have been doing virtually through closed groups), had the distinct advantage of each winner being able to spend considerable time interacting with jury and among themselves with no other formal programs beyond the awards, CIO talks and interactions.

In Delhi, the ceremony was held at Vivanta by Taj, Ambassador on Thursday, 27th February 2020. Anchored by Shyamanuja Das, Managing Editor, 9.9 Group, three jury members—Vinod Sivarama Krishnan, Chief Information Officer, IndusTowers; Biswanath Ghosh, CIO - Enterprise & Corporate Functions, Mahindra&Mahindra and Sachin Gupta, President & Chief Information & Innovation Officer, Usha—giving away the awards and speaking to the awardees.

In Mumbai, the awards ceremony was hosted at Sofitel BKC on Friday, 28th February 2020. Anchored by Vikas Gupta, Co-Founder & Director, 9.9 Group, there were insightful talks by Jury members, Narayanan Ramakrishnan, Executive Director - Information Systems, BPCL; Subhash Shelke, CIO - Corporate Services & Head -Applications Delivery, Essar Group; Rajeev Jorapur, Senior Vice President, Bajaj Auto; Amandeep Singh, Vice President - Technology, Thomas Cook India and Nirupmay Kumar, Senior Vice President - IT, Vodafone Idea. The jury members also handed over the awards.

R Giridhar, Group Editor, 9.9 Group, anchored the Bengaluru award ceremony, held in The Park Hotel, which saw Ashvin Vellody, Partner, Deloitte Digital, and Jury member, Ramakrishnan Sudarshanam, Divisional Vice President - IT, United Breweries, giving away the awards and speaking to the awardees.

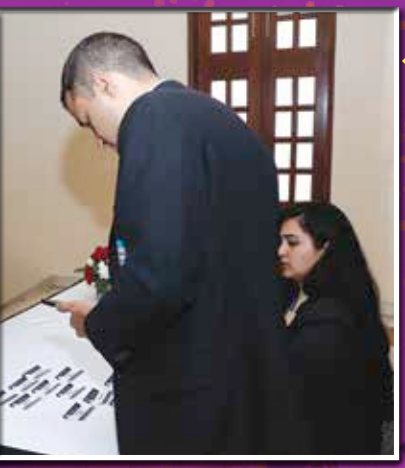
Have a look at the ceremonies through a pictorial presentation in the next few pages.

DELHI

NEXT100 Delhi Winners - All in one frame

Jury member, Vinod Sivarama Krishnan, Chief Information Officer, Indus Towers presenting the opening address

Inspiring talk by Jury member, Sachin Gupta, President & Chief Information & Innovation Officer, Usha



NEXT100 Delhi:
Catching up with 9.9ers

Jury member, Biswanath Ghosh, CIO - Enterprise & Corporate Functions, Mahindra & Mahindra presenting his talk

Shyamanuja Das, Managing Editor, 9.9 Group anchoring the event

The audience in rapt attention...

Winners networking over Hi-Tea

MUMBAI

NEXT100 2019 Mumbai Winners - Posing happily!

Vikas Gupta, Co-Founder & Director, 9.9 Group anchoring the event

Jury member, Amandeep Singh, Vice President - Technology, Thomas Cook India presenting his talk

Jury member, Nirupmay Kumar, Senior Vice President - IT, Vodafone Idea delivering an interesting speech

Jury member, Narayanan Ramakrishnan, Executive Director - Information Systems, BPCL: The opening speaker at the event

Jury member, Subhash Shelke, CIO - Corporate Services & Head - Applications Delivery, Essar Group speaking at the event

An insightful talk by Jury member, Rajeev Jorapur, Senior Vice President, Bajaj Auto

NEXT100 2019 Book being unveiled by the Jury members

BENGALURU

NEXT100 Bengaluru Winners with the Jury - All Smiles!

R Giridhar, Group Editor, 9.9 Group anchoring the event

Winners enjoying some Refreshments

Ashvin Vellody, Partner, Deloitte Digital presenting his opening talk at the event

A good platform for winners to interact

An insightful talk by Jury Member, Ramakrishnan Sudarshanam, Divisional Vice President - IT, United Breweries

Audience listening attentively

NEXT100 Winner Trophies

What Exactly Is A Data Center Park?

And why should it matter to you?

By Shyamanuja Das

Even though the draft Personal Data Protection Bill has been referred to a House Select Committee, the Government of India has made its intention clear that data localization (one copy of all data must stay within the shores of India) requirements will stay.

Data center parks in public-private partnership (PPP) announced by the finance minister Nirmala Sitharaman in her budget speech is probably meant to ensure that businesses find this proposition economically viable. It will not be surprising if further incentives announced for locating data centers within designated data center parks, much in the same line as manufacturing SEZs or Software SEZs/STPs.

"It is now a cliché – "data is the new oil" and it is true that Analytics, Fintech and Internet of Things (IoT) are changing the way we deal with our lives," said the minister in her speech.

"To take advantage of this, I propose to bring out soon a policy to enable

private sector to build Data Center parks throughout the country. It will enable our firms to skilfully incorporate data in every step of their value chains," she added.

The objection to data localization requirements in the draft Personal Data Protection Bill is from two quarters—the activists and the corporates. For the first set, it is a question of freedom; the second set—which the government wants to address—had reservations primarily, if not only, because of commercial reasons.

The establishment of data center parks—with some possible incentives to locate a data center in it—is one way of addressing those concerns.

The objective seems to be threefold:

1. Minimize the opposition to data localization requirements by businesses by making the local data centers far more viable economically.
2. Make it attractive for small businesses to host their data in well-managed, world class data centers. This goes well with the government's thrust on MSMEs and digital India.
3. Make India a favored destination for global data centers, as the demand explodes. If the hyperscale providers find it attractive, much of the opposition to data localization will go anyway.

Already on the anvil...

Even before the FM's announcement, there have been movements on establishing data center parks by infrastructure companies.

Maharashtra Industrial Development Corporation (MIDC) announced in October 2019 the establishment of a data center park in the Taloja Industrial Estate in Navi Mumbai. The park will be built in two phases, with the first phase involving an investment of INR 30,000 crores, with half of that coming as FDI. The second phase of the park, to come at Khalapur, will be on a land of 500 acres.

Around the same time, the Adani Group announced its foray into the data center domain, in partnership with San Francisco-based Digital Realty a global provider of data center, colocation and interconnection solutions.

As and when the data center parks—even in a limited manner in major cities—become a reality, the enterprise IT managers have to calculate the new economics...

In July 2019, Hiranandani, a Mumbai-based real estate developer also formed a data center company, Yotta, to set up data centers, beginning with Mumbai, Chennai and Panvel in Raigad district of Maharashtra.

The Challenges

All these data centers that MIDC, Adani Group and Hiranandani have announced are expected to cater to the big Indian businesses and global businesses. But if the government really wants to democratize setting up of data center parks—so that their services can be availed by a large section of medium to small enterprises—they have to come up across the country.

While information technology is not a challenge, basic infrastructural challenges do remain.

First—but arguably the easiest to tackle—is the real estate. The fact that big real estate owners like MIDC and Hiranandani have entered the space, is a testimony to this assumption.

Second is connectivity. While seamless connectivity is a challenge in many areas, it can also be tackled by a focused plan.

By far, the most important challenge is quality power availability. Even today, there are many areas with challenge in good power availability. If the data center parks have to be established beyond the metros and big cities, making good power available will have to be a top priority.

"This partnership," said Gautam Adani, chairman of Adani Group while announcing the Digital Reality partnership, "leverages several of the capabilities developed by the Adani Group in power generation, transmission, retail electricity distribution, access to waterfronts through the ports business, and real estate management. Also, as one of the top five renewable energy companies in the world, our ability to power our data centers with solar and wind energy is unique and addresses some of the challenges of building and operating data centers."

Adani's stress on his company's strength in generating and distributing power is a good way to gauge how critical it is for data centers.

Hirandanani also has its own solar power plant and distribution. Even data center companies like NTT Netmagic have ventured to set up their own solar power centers.

Data center parks across the country is a good idea to start with. But the challenges of power and connectivity must be addressed before it becomes a widespread reality.

The IT Infra Manager's Choice

As and when the data center parks—even in a limited manner in major cities—become a reality, the enterprise IT managers have to calculate the new economics—either of moving to a captive/hosted data center or negotiating a better cost structure with large cloud service providers.

But the commercials can be worked out only when more details around the government policies/rules on data center parks become available, including incentives, if any.

However, all CIOs and IT infrastructure heads should keep this new reality in mind while doing long-term investment and delivery model planning for their IT infrastructure. ■

Disruptive Changes & Regulatory Pragmatism

Apart from bridging the gap between regulations and changes in business environment, pragmatist regimes should ensure effective implementation and strict monitoring

By Anthony Crasto

In today's regulatory environment, technological advancements are bringing in change at a rapid pace. Regulators and businesses are challenged to maintain a balance between fostering innovation, enforcing regulation, and addressing the unintended consequences of disruption. Technology and digital interventions, and easy access to low cost bandwidth, has been disrupting business models, as also how products and services are produced, delivered and consumed.

In such an evolving environment, it is imperative that regulations keep pace, ensuring appropriate balance between the needs of society, business and state. Historically, we have seen a time lag between emergence of new business models based on disruptive technologies and enactment of regulatory policies governing them. If we look at it from a consumer perspective, the benefits of these disruptive technologies are very high, since they provide instant service and a high level of consumer satisfaction. However, over a period of time, due to various negative instances, the need to regulate these technology innovations is required for protecting consumer interests and safety.

We can think of these disruptions and need for regulation to keep pace in various categories.

A) Convergence of business models

Technology has created a high level of business convergence and lines between traditional business definitions are either getting blurred or fading away. Telecom companies are now defining their business as technology communications rather than only telecom. Technology companies are now in the consumer travel and hospitality business.

As business models converge, regulators need to keep pace with defining regulations and policies towards these innovative models. Globally too, there are no unified or well-defined policies and regulations to these innovative service delivery models. The Industry is developing, or has developed, self-regulating policies for companies to follow.

Some of the examples include the significant increase of online media streaming and consumer viewing. The influx of smartphones and easy access to data has significantly increased the scale at which such online media is easily available. Currently, most of the online content is self-regulated and not covered by any national regulation.

The other example is in terms of policy governing the e-commerce industry. In the last 5 years, the boom in e-commerce has been significant, with some large global and Indian players leading the India market.

The e-commerce industry, which has a high future potential and aims to significantly grow to USD 200 billion by 2026, has led to the government releasing the draft National e-commerce policy in 2019. The government plans to issue this final policy in the near future.

Regulators need to also focus on introducing regulations for certain industry-specific e-commerce businesses, such as e-pharmacy, which can have a serious impact on public health and safety if left unregulated.

B) Social media, mobile apps/digital interface with consumers/general public

Companies use social media sites, mobile apps and create various digital interfaces to reach out to the consumers/general public, gather significant amount of personal and consumer data. Such data invariably includes personal data of an individual, as also of his/her preferences. The growing use of internet-connected devices has created a vast digital footprint - a trend that is only set to accelerate.

Globally, and in India, various instances have been reported of data breaches of personal data, data being used for ulterior objectives, unauthorized transfer of data across jurisdictions, leakage of personal data, etc. Considering these issues, various countries have now started releasing new and/or updating existing policies and regulations to address these emerging risks on how consumer data is collected, stored, processed and used.

It is important that regulators understand the risks associated with technology disruptions...

However, despite the amount of data generated, nearly 30% of nations have no data protections laws, and those that do, lack uniformity. It is important that regulators understand the risks associated with technology disruptions in a proactive manner and work with the industry and industry associations to define regulations which assist in protecting consumer/public interests.

C) Increasing focus on consumer experience and safety in case of traditional business

The increasing focus on consumer experience and safety is driving regulators to focus on enhancing regulations with respect to these sectors. For example, if we take the education sector, there has been significant growth in private schools, play schools, etc. However, regulations pertaining to student safety require further evolution.

In case of the healthcare industry, the use of technology is increasing significantly and a significant amount of sensitive patient data is collected, stored, and analyzed. IoT technologies are being implemented and even surgeries are being done through robots. Considering these technological interventions, it is important for regulators to understand the risks associated with these technology advancements and introduce regulations which will protect public interests and safety.

Endnote

Protecting consumer and public safety and interests is one of the paramount objectives of regulators. Considering the rapid change in business models, they too, will need to evolve at a rapid pace and proactively anticipate risks which may impact consumer/public interest, and introduce appropriate regulations to protect them.

As of now, there seems to be some lag between evolution and maturity of regulations as compared to changes in the business environment. It may be noted that regulation alone will not solve issues, effective implementation and strict monitoring are required if we need to make regulations, polices and legislations effective.

The most important objective is protecting consumer interests and at the same time driving positive consumer experience. To that effect, corporates also have an important role to play. As they continue to innovate and evolve newer business models, they too need to consider the implications this might have in safeguarding the rights of citizens and society. They are, after all, the target consumers of the company's products and services and having a *laissez faire* approach to this aspect could impact the brand and reputation of the organization. ■

The author is Partner, Deloitte India

Using AI As An Adaptive Immune System For Networks Against Cyberthreats

In the network, AI can identify threats and initiate and coordinate a response

By Rajesh Maurya

Imagine what you would have done differently in your network if you could have just seen a few years into the future. Would you have been quicker to embrace the cloud? What about the time and money spent on technologies that you now don't really use? Every wiring closet has a number of expensive boat anchors sitting on a shelf somewhere gathering dust. Of course, if your organization has ever been the victim of a serious breach, it's easy to guess how you may have prepared differently for that.

Predicting the Future

The truth is, that last one isn't really just wishful thinking. Cybersecurity professionals have been warning organizations about the threats just around the corner for years. Some require years of experience to understand threat actor trends and malware trajectories. But others just stare you in the face. For example, much of the recent success of the cybercriminal community has been due to their ability to successfully exploit the expanding attack surface and the resulting security gaps resulting from digital transformation that are not being properly closed. This shouldn't be news to anyone.

While predicting what cybercriminals are going to do next can be tricky, the reverse isn't true. When it comes to the cyber arms race, the criminal community has always had a distinct advantage in knowing what's coming next. Organizations are constantly looking for new ways to squeeze more value out of their networks, or gain that sliver of competitive edge through the use of new technologies. And cybercriminals can predict with a high degree of certainty where many of those organizations will also neglect to apply proper security to those efforts.

According to one report, cybercriminals cost the global economy a total of USD 1.5 trillion last year. And the rate of growth for cybercrime looks likely to continue for some time unless organizations make a significant paradigm shift as to how they think about and deploy security.

Gaining the Upper Hand

To get out ahead of the traditional cycle of buying new cybersecurity solutions in response to the latest threat trends, organizations need to begin using the same sorts of technologies and strategies to defend their networks that criminals are using to compromise them. That means

adopting an intelligently integrated approach that leverages the power and resources of today's enterprise.

Much of this is detailed in a Fortinet's Security Predictions report for 2020. In addition to our predictions around the tactics and technologies that cybercriminals are likely to develop and adopt over the next few years, this year's report focuses extensively on ways organizations can successfully gain the upper hand when it comes to their cyber adversaries. And that strategy relies heavily on two things: The development and deployment of solutions built around machine learning and artificial intelligence, and shifting to a security-driven networking strategy that takes the principle of "look before you leap" to a new level.

The Evolution and Future of AI

One of the objectives for a security-focused AI strategy is to develop an adaptive immune system for the network similar to the one in the human body. In the body, white blood cells come to the rescue when a problem is detected, acting autonomously to fight infection. In the network, Artificial Intelligence can potentially perform much the same task by identifying threats and initiating and coordinating a response. A quick review of its history can help us predict its trajectory.

The first generation of AI is already in place in some sectors. Leveraging artificial neural networks and massive databases, systems using machine learning can rapidly sift through mountains of data to provide analysis and determine a proper course of action, all at network speeds.

The next generation of AI, currently running in labs and some production environments, is better able to detect patterns by distributing learning nodes across an environment. This enhances its impact on things like access control. Some AI systems are now able to identify individuals using complex bio-footprints, such as typing patterns or heartbeat rhythms, and detect even the most subtle deviations in normal network traffic to identify malicious actors and malware. Implementing this in today's networks will require deploying regional AI-enhanced learning nodes that can collect and process local data for quick responses to events, and also share that data back to a central AI brain to deeper correlation to not only better detect suspicious patterns of behavior, but also immediately respond in a decisive manner before an attack can even be fully formed.

The third generation of AI, however, is where things begin to get really interesting. AI will still require a central brain, but rather than a hub and spoke model, it will instead exist as an interconnected web of even more intelligent regional learner nodes, much like an organic neural network.

The third generation of Artificial Intelligence, however, is where things begin to get really interesting

Direct information sharing between nodes will not only play a pivotal role in identifying threats in true real time, but also ensure that central protections and controls match local requirements and variations.

Getting from Here to There

Of course, none of this will matter if security isn't deployed where cybercriminals strike. Today, different segments of the networks can't see or talk to each other and collected threat intelligence often exists in isolation. The result is a fragmented security implementation that cybercriminals are all too eager to exploit. And this challenge is being compounded as more and more organizations rush headlong into adopting new technologies – today it's the cloud and tomorrow it will be 5G and edge computing – without first properly considering all of the security ramifications. And that has to include prioritizing how the security to be deployed in new areas of the network will interoperate with existing systems.

Getting from where most organizations are today, to the sort of integrated and distributed security that the future will require, underscores the need to take a new approach. To start, organizations need to focus on interconnectivity and deep integration between their security devices. For machine learning systems to be successful, they not only need access to critical security information, but that data will need to be seamlessly and instantly shared across the network so can be adapted to each networked environment's unique configuration. This will also require taking a security-first approach to new network expansions to ensure that all network and security systems and devices are visible and consistently controllable from anywhere in the network.

The ability for machine learning and AI systems to take over many of the menial and detail-oriented tasks previously assigned to human resources will take a significant bite out of the growing cybersecurity skills gap. By shifting responsibilities to autonomous self-learning processes, that function similarly to human autoimmune systems – hunting for, detecting, and responding to security events autonomously and in true real-time – valuable cybersecurity professionals will be able to focus their unique skillsets on higher-order planning and strategy. This transition will be critical as organizations move to adopt the advanced security-driven network strategies that will help their businesses succeed in the digital marketplace of tomorrow. ■

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

Phishing Now A Year-Round 'Sport'

It is no longer confined to shopping seasons

By Santosh Matam

Phishing attacks have been a leading cause for breaches globally, with 83% of information security (infosec) professionals reported having experienced phishing attacks in 2018, up from 76% in 2017, according to Proofpoint. This upward trajectory is due to the ease with which threat actors can launch these attacks. As opposed to hacking through a firewall, deciphering encryption or finding a vulnerability within your system, a good trick email pitch and a fake landing website are all that is needed to launch an attack.

Cybercriminals Love the shopping season!

Shopping season is tricky for consumers, and exciting for cybercriminals. Many ramp up online shopping in the lead-up to the holiday period and, as their 'to-do' lists get longer, some will inevitably let their guard down online. Cybercriminals know this too well

and they consequently spend a lot of effort devising schemes to take advantage of such corner cutting behavior.

According to reports, 56.1% Indians have fallen victim to discount scams by clicking on malicious links during holiday shopping online this year. While cybercriminal activity continues to grow in sophistication, popular scams like email phishing (25.3%) and text phishing (21.1%) still result in close to a quarter of Indians being duped throughout the season.

Phishing attacks used to be a popular attack vector during the holiday season as it is easier to trick people into opening notifications for package deliveries or receipt emails from their online shopping spree but now this pattern has changed. The rise of social media makes personal data freely available to attackers anytime. They no longer have to wait for the year-end holiday shopping season to trick unsuspecting shoppers. This means that phishing has now become a year-round sport, making it a definite concern for businesses and individuals alike.

56.1% Indians have fallen victim to discount scams by clicking on malicious links during holiday shopping online this year

The anatomy of the "phish"

While most of us are aware of the concept and pitfalls of phishing attacks, attackers are still able to easily launch phishing attacks by preying on human behavior. These scams continue to work so well because they appear legitimate to users. By using the names of friends and colleagues—information that is relatively easy to come by through an analysis of social media accounts or via open source intel and spam lists—and by leveraging popular brands (Facebook, Microsoft, Amazon, Netflix and Apple), hackers are able to get users to lower their guard.

Furthermore, phishing emails continue to be effective because they are three times more likely to have a malicious link than a harmful attachment. These links tempt users to click on them to find out more. They, of course, lead to fake websites designed to harvest credentials, trick users into installing malware, or inject virus into the vulnerabilities found in browsers. To make such scams look even more legitimate, 71% of phishing sites use HTTPS, while 85% feature certificates by trusted authorities.

How to avoid falling for phishing attacks?

There are many ways to prevent your organizations from falling prey to these phishing scams. Coupled with awareness training and guidance on how to assess the legitimacy of emails and other types of phishing methods, organizations can also ensure incoming emails from external sources are clearly labeled to prevent spoofing.

Users should slow down and validate offers before clicking on any links, and as always, exercise more caution when required to input their personal data anywhere. Any too-good-to-be-true offers featured in popups and links need to be viewed with extra scrutiny.

Furthermore, apart from relying on regularly updated anti-virus software to stop malware installation attempts, IT teams should install a web filtering solution to prevent users from inadvertently visiting phishing sites—a handy defense tool to the anti-phishing arsenal.

Multifactor Authentication (MFA) is another phishing "gap insurance" that prevents stolen credentials from being used from an unexpected location or unknown device.

Finally, with more than 90% of internet traffic encrypted and 68% of malware phoning home through encrypted tunnels, IT teams also need to deploy a decryption gateway before sending through to incident detection tools to detect infections.

By implementing these steps, it becomes difficult for threat actors looking for an easy way to make a quick buck where the game is all about low effort for high yields. ■

The author is Security Manager, India, F5 Networks

The Role Of AI In Cybersecurity - Boon Or Bane?

The global market for AI cybersecurity is projected to grow at an astounding compound annual growth rate of 36% to reach USD 18.1 billion by 2023

By Murali Urs

Reliance on Artificial Intelligence (AI) to combat cybersecurity threats is forecasted to increase by several orders of magnitude over the next five years. A report from P&S Market Research says the global market for AI cybersecurity is projected to grow at an astounding compound annual growth rate of 36% to reach USD 18.1 billion by 2023. Due to the fast-paced digitization, organizations are increasingly under attack by malicious bots. Unfortunately, most web application firewalls don't provide enough bot mitigation capabilities. There has been a new wave of industry growth, investment,

and innovation, as a response to ever more targeted and sophisticated social-engineering attacks.

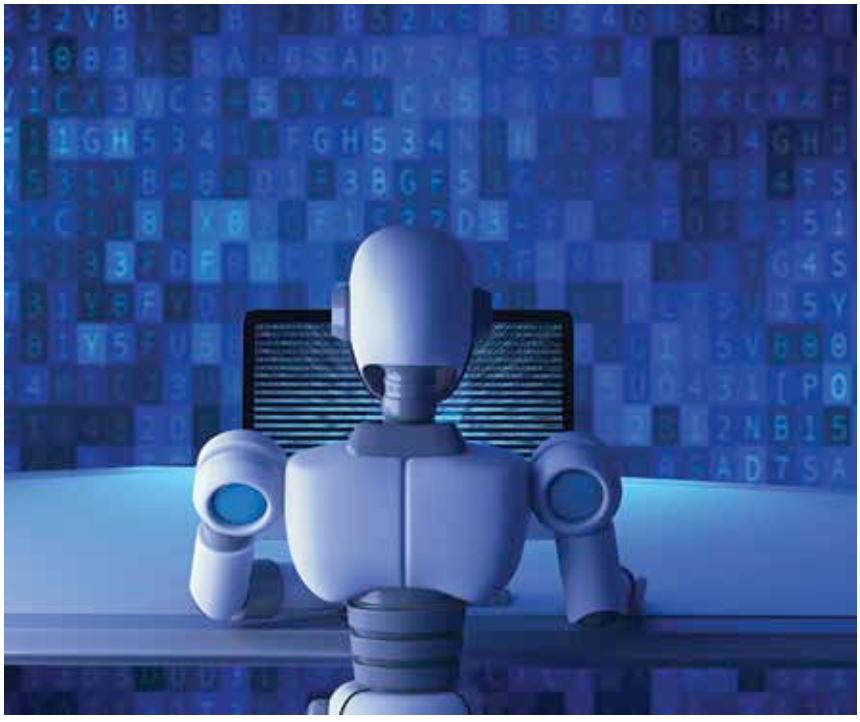
Cybercriminals have shifted their business model: Instead of casting a wide net and hoping that one in a million email recipients will fall for the scam, they launch targeted attacks against larger organizations to monetize with much greater payoffs. With antivirus solutions stopping spam and viruses, attackers started writing custom zero-day malware that could evade traditional anti-viruses. Soon, attackers realized that people are the weakest link in the chain and started launching phishing and ransomware attacks to effectively monetize their efforts. Attackers go to great lengths to personalize a message that will earn the trust of the recipient.

Defending against attacks launched using AI models is, of course, going to require organizations to have access to AI models of their own to defend their organizations. To stop impersonation, one must understand internal patterns, who's talking to whom, when, how frequently, is the conversation typically one way or not, which email addresses are they using, etc. An AI engine ingests many signals related to the metadata of the message (who's sending to whom) and its content, which allows it to determine with a high degree of certainty whether the message in question is spear phishing. The AI engine is powerful because it identifies impersonation attempts and stops the attacks in real-time. It also gives a view into those individuals who are at the highest risk of both being impersonated and being targeted.

The trouble is that building these AI models not only takes a lot of time and effort, it also requires organizations to have access to massive amounts of data to teach the machine and deep learning algorithms employed to create the AI model to recognize cybersecurity attacks. More challenging still, as the cybersecurity attacks evolve, those AI models need to be constantly updated. AI applications are only as good as the algorithms on which they are based. Those algorithms require access to massive amounts of data to identify patterns. It should combine three dedicated layers of defense:

- Artificial Intelligence (AI) Real-Time Spear Phishing Prevention
- Domain Fraud Visibility and Protection
- Anti-Fraud User Training

AI is paradoxical, while it is upgrading cybersecurity, cybercriminals already have the bots required to collect the data required to build AI models. They can also afford to recruit the expertise needed to build AI models. If it persists, AI can accelerate havoc and become perilous to cybersecurity. As it is still growing, its potential is incomprehensible, we cannot be certain that it will be helpful or adverse for cyber security. In theory, at least, the overall state of cybersecurity should improve. Simultaneously, it's important that enterprises do as much as they can by combining the AI & conventional approaches to safeguard their organizations. ■



AI is paradoxical, while it is upgrading cybersecurity, cybercriminals already have the bots required to collect the data required to build AI models. They can also afford to recruit the expertise needed to build AI models. If it persists, AI can accelerate havoc and become perilous to cybersecurity

The author is Country Manager, Barracuda Networks

Next-Gen Authentication In Indian Digital Payment Infrastructure

Aadhaar/Biometric Authentication and Time-based Multi-factor Authentication can transform the Indian digital payment system

By Vishal Kumar

Mobile/IoT devices are increasing day-by-day and digital payment industry is also at the peak. IoT and mobile devices has a great impact on human lives, it is penetrating numerous aspects in human lives by obtrusively working in the background without making realizing its presence for us. IoT devices are everywhere near us these days which includes smart cars, drones, health monitors, doors, windows, fans, TVs, refrigerators and electronics appliances in a smart home, smartwatches, etc. All these IoT based devices can easily be operated with the help of mobile applications. Most of digital payment apps, messaging apps are also on mobile devices or IoT devices. With the growing popularity of Mobile and IoT technology and increased demand for connected devices, cyber criminals are also increasing day-by-day and current authentication and infrastructure is not much capable to track cyber criminals.

So what's next in Payment industry to track and reduce Cyber Crime?

- **Biometric Authentication to reduce Cyber Crime:** Considering the spectrum of law enforcement, biometric authentication can play a key role to stop and track cyber criminals. This solution enables law enforcement agencies to identify cyber criminals through their physical or behavioral characteristical biometric data. Moreover, fingerprint sensors, face recognition, Iris scan are also significantly emerging as the latest trends in providing civil identity, voter registration and population registration.
- **Aadhaar/ Biometric Authentication in Indian Payment Infra:** Aadhaar Authentication provides a digital, online identity platform so that the identity of Aadhaar number holders can be validated instantly anywhere at any point of time. Aadhaar-based authentication

as a service can be utilized by the requesting entities to authenticate the identity of the users based on the match of their personal identity information before providing them access to their services or business functions. Providing services through information technology infrastructure creates a great impact in organizations. To expand the reach of these organizations, verifying an individual's identity fulfils an important aspect of security.

Who should move to this Solution and help nation to reduce Cyber Crime?

Finance companies, Mobile Payment Apps, Public & Private sector Banks and all Digital Payment industry should start moving in the direction of biometric authentication as a 2nd level authentication mechanism. Authentication remains one of security's biggest concern in today's fast growing scale of cyber crimes. Using multiple factors in authentication mechanism, makes the authentication more stronger and reliable by adding additional layers of security.

Techniques to Control Cyber Frauds: An example of Next-Gen E-Wallet to E-Wallet transaction:

Biometric authentication can play an important role in reduction of cyber crime and can control E-wallet and digital transaction frauds to a greater extent. In this biometric authentication mechanism, the sending party and receiving party will use biometric authentication in their process of digital transaction. This transaction process will help the concerned authority to track or record digital money, which in return will be helpful to catch cyber frauds. Hence, reducing the statistics of cyber frauds involved in these E-wallet and digital transaction process to a significantly greater extent.

Let us understand: The workflow and concerned postulates involved in the biometric authentication mechanism in this digital transaction process considering Paytm as an E-Wallet.

Step 1: Paytm User A (Sending party) will be transferring digital money to Paytm User B (Receiving party).

Step 2: 1st authentication process involved for User A is the PIN and the 2nd authentication process is his biometric authentication from the Aadhaar.

Step 3: The Receiving party, User B will have the PIN as his 1st authentication process and the biometric authentication as the 2nd authentication process to verify funds.

Step 4: Now, the User B will virtually receive the money transferred from User A, with his PIN. But, in order to use the money, User B will have to process biometric authentication through Aadhaar linked with his account.

Time-Based Multi-Factor Authentication:

This approach uses a secret shared between the server and the client (typically a mobile app) in conjunction with the current time to generate a one-time use code. The client knows the code by running the shared secret through the algorithm. The server can verify the posted code by running the same secret through the algorithm. The code is only valid for a set amount of time, usually 30 seconds.

The flow looks like this:

1. You log into an application with your username and password.
2. You see a text field, asking you to input the latest code.
3. You launch your TOTP client on your mobile phone and see the current code.
4. You enter the code in the text field and proceed on to the application.

It's more secure than the SMS approach, because there is no medium of transmission for the code. It is generated by the algorithm. The shared secret must be kept a secret for this approach to remain secure.

One of the most popular implementations is the Google Authenticator. It makes the TOTP approach easier to use by showing the secret as a QR code that most mobile apps can read. This is much more reliable and easier to use than the manual input of a shared secret.

Benefits Involved and Need of Hour in Country to make Payment Infra Secure

- Receiving party and sending party is under biometric surveillance and Govt, Police and national forces can track any cyber crime, which is happening through banks/wallets and E-banking.
- Reduction in Cyber Crime and easier tracking of Cyber criminals and frauds.
- Need of hour to prevent financial infra/consumers with next gen level authentication solution.
- Digital Money transaction tracking or record becomes simpler, flexible and reliable.
- Tax benefits to government involved in these digital transaction process.
- 99% reduction in Cyber Crime in the Payment industry, improves security and reduces the risk of an intruder gaining access to critical financial systems and data.
- Reduction in the state of corruption to a greater extent.

Challenges Involved but Achievable:

- Potential cost increase for things like additional support, training, maintenance, SMS Gateway or services, hardware and software tokens.
- Infrastructure upgrade for the Mobile system, Data centers and secure backend & frontend code review for the application.
- Good Internet-connectivity and bandwidth within the Country.
- Encouragement of Cyber Awareness to the Consumers through Cyber Security awareness campaign, seminars, training, etc. ■

The author is LLB, LLM (Cyber Laws)

Emerging Role Of Artificial Intelligence In Social Sector

From improving crisis response to improving crop yields: Artificial Intelligence is set to play an increasingly impactful role in the social sector

By Tuhin Banik

Artificial Intelligence is already impacting our lives in a major way. Be it getting driving instructions through our smart phone or getting daily reminders by our fitness device to increase our workouts, all these are manifestations of how Artificial Intelligence is changing the way we function. What is often less understood is the significant role Artificial Intelligence can play in the social sector.

Artificial Intelligence can potentially help solve some of the country's most pressing problems. As a matter of fact, it can contribute in some way or another to tackling all of the United Nation's Sustainable Development Goals, helping large sections of the population in both developing and developed countries. AI is already being applied in a number of real life situations, from helping blind people navigate and diagnosing cancer to identifying sexual harassment victims and helping with disaster relief.

Let us take a look at critical social domains where AI can be implemented effectively:

- **Crisis response** - Rainier Mallol, a scientist from the Dominican Republic, was successfully able to predict dengue outbreaks three months in advance with up to 81% accuracy after feeding statistics of previous outbreaks to an AI algorithm. This successful harnessing of big data to predict deadly diseases can remarkably change the way we address epidemics. There are a number of crisis specific challenges, such as relief response to man-made and natural disasters, especially rescue missions and disease outbreaks. AI can be applied on satellite data to predict wildfire progressions and optimize the control reponse. AI can be used in conjunction with drones to look for missing persons in the wilderness.
- **Precision agriculture** - AI can help farmers analyze a variety of factors, such as temperature, weather conditions, soil conditions and water usage, in real time. It can be used to optimize planning and generate a more bountiful yield by determining the best crop choices and the most optimal way to utilize resources. AI has been effectively deployed to detect crop damage with the help of low-attitude sensors, from drones to smartphones, to improve the crop yield of small farms.
- **Educational challenges** - AI can be used to maximize the achievement of students and the productivity of teachers. Adaptive teaching technologies can be used to recommend content and courses to students based on their engagement and success with past courses and material.
- **Environmental challenges** - To sustain biodiversity and combat climate change, pollution and the degradation of natural resources. Rainforest Connection, a non-profit organization located in the Bay Area, uses AI tools like TensorFlow to conserve fragile rainforest ecosystems around the globe. By analyzing the audio-sensor data in vulnerable areas, we can successfully detect and prevent illegal logging activity.
- **Inclusiveness and equality** - This would seem like a far-fetched connection but AI based technology also has the potential to improve social inclusiveness and fight discriminatory tendencies by using and analyzing big data. A good case study is Affectiva, a combined effort by the media lab at MIT and the Autism Glass Project that makes use of AI to automate emotion recognition and provide helpful social cues to help people at different stages of the autism spectrum to interact better in social settings. Addressing challenges related to inclusiveness, equality, and self-determination are some of the most pertinent issues in this domain. These include reducing bias based on religion, race, sexual orientation, disabilities and citizenship.

Addressing challenges related to inclusiveness, equality, and self-determination are some of the most pertinent issues in this domain

- **Healthcare** - Early diagnosis of diseases is another area where AI can help for the better. Researchers at Stanford University and the University of Heidelberg have created an AI based system for detecting diseases. They found that AI based image processing software were able to scan images of lesions and determine whether they were cancerous more effectively than professional dermatologists. By interpreting the heart rate sensor data, wearable devices with AI powered software can detect people prone to diabetes with up to 85 percent accuracy. If they are made more affordable, they can help over 400 million people globally.
- **Information validation** - With the fake news epidemic growing direr by the day, we need systems to facilitate provision and validation of reliable, helpful and valuable information to the masses. We need to focus on counteracting or filtering distorted and misleading content, including false information peddled on social media, internet and messaging applications. Malicious and false content can have severe negative consequences, from the manipulation of election results to mob lynchings. AI can contribute to this domain by presenting counteractive views to the ideologically insulated pockets across social media platforms.
- **Infrastructure management** - AI can also help with infrastructure challenges and promote public good in the power sector, waste and water management, real estate, urban planning and transportation. For instance, traffic light control systems can be optimized with the help of real time footage and Internet of Things sensors to maximize the passage of vehicles through crowded areas. AI systems can be used to schedule maintenance of public transport systems, from trains to public infrastructure, and identify malfunctioning components.

These are just a few areas in which AI can help address important challenges. While the potential for its use is immense, scaling it up will need focus, funding and concerted efforts from the different stakeholders to work for the benefit of mankind. ■

The author is Founder, Thatware LLP

How To Get Your Data Management Strategy Right In 2020?

A multi-cloud strategy or cloud-adjacent model can address your data management issues

By Srikanth Doranadula

Did you know? 90% of the world's data today got created just in the last two years. In the digital economy, organizations are trying to manage burgeoning data, while simultaneously trying to extract actionable insights to unlock new business growth. With data emerging as the new catalyst for innovation, organizations are racing against time to transform themselves into data-driven businesses.

In the era of Industry 4.0, organizations can no longer afford to have their data locked up in separate siloes across the hybrid IT estate. As per a recent Forrester research, 73% organizations still have disparate and siloed data strategies in place, and 64% are challenged with a multi-hybrid infrastructure. It's little surprise therefore that 70% of these organizations attribute process simplification as a high or critical business priority.

Can a multi-cloud strategy help?

As organizations realize the need to break down these siloes and better streamline their business, the public cloud is a good option to consider. However, a 'one-size fits all' approach will not work. More and more organizations are now considering a multi-cloud approach, because of the choice for them and their application developers to pick and choose components from multiple cloud providers, using what's best for their use case. Research validates this trend, with nearly 3 out of 4 organizations expecting to use a multi-cloud model in the next couple of years.

For organizations looking to become more data-driven by using their data as an innovation engine, the capability to be selective is crucial. Because it can help them to move key corporate data closer to vital cloud services, such as high performance compute and new services that enable access to emerging technologies like Artificial Intelligence (AI), Machine Learning (ML), and advanced analytics helping them develop new business models.

Time to consider a different approach to cloud?

For some organizations still hesitant to explore the public cloud via a cloud-first or a cloud-only model, there's one more path to get cloud-ready, while still enjoying the benefits of a public cloud like environment. This 'Cloud Adjacent Architecture' offer you the elasticity of the cloud along with the processing power of on-premise IT.

In effect, such a model puts an organization's data on powerful cloud-ready infrastructure close to the public cloud across a globally interconnected exchange of data centers. This then enables organizations to interconnect securely to the cloud, as well as other business partners, while also directly reducing networking costs as well as latency.

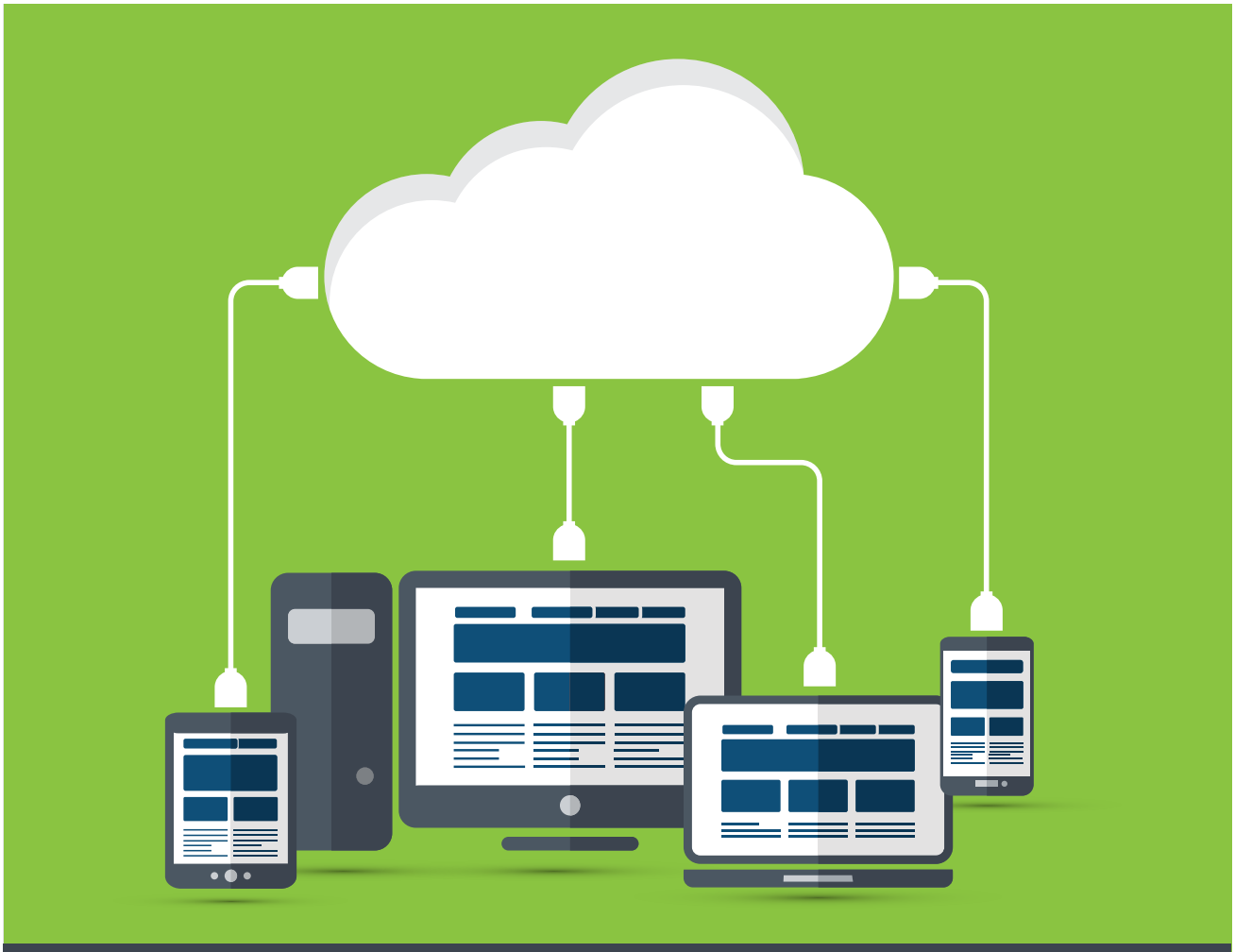
The benefits of such an approach are immense. Enterprises can reduce their data center footprint, take advantage of the scale and variety of modern public cloud services, while still retaining the precision, data ownership and control of an on-premise IT setup.

Furthermore, this 'Cloud Adjacent Model' can offer a zero-change architecture - which means, companies need to change nothing. What's another good aspect is that customers get to choose who manages the data and how, providing total flexibility. This additional flexibility to multi-cloud architectures can help support the push towards digital transformation.

Take smart city initiatives for example, involving a large number of cameras, sensors and the like. The convergence of the digital and physical worlds provides those driving smart city initiatives a unique opportunity to understand better the dynamics of a location on a real-time basis and then use insight to provide value back to residents and businesses via provisioning new or better services, often delivered via an app.

This new approach combines the best of both worlds within a multi-cloud model, potentially eliminating some of the core drawbacks of data complexity, and helping usher in more project rollouts faster - to ultimately make a significant difference to citizens' lives. ■

The author is Senior Director & Head - Systems Business, Oracle India



A Realistic ASaaSement

In contrast to infrastructure, where the cloud takeover is now complete and unquestionable, software-as-a-service has been able to secure less than one-fourth of the enterprise software spend. What does it say?

By Shyamanuja Das

In the initial days of Software as a Service (SaaS), one of its biggest attractions was that it allowed the non-IT functional executives to invest in the solutions that solved their problems well—and without involving the IT department.

It provided three great value propositions.

One, it changed software from a capital expenditure to operational expenditure. That meant the decision could be taken at the SBU/division level, rather than waiting for the central IT/finance to approve the Capex. Capex decisions are almost always centralized and far more bureaucratic than operational spends.

Two, most of the initial SaaS companies understood the problem statement of these business units much

better and so their solutions were far more appropriate. That meant saving on a lot of time and hard work of explaining to the IT guys—who, at that time, understood very little of business language.

Three, it did not require any expertise from the internal IT guys and hence could be bought, installed and run without their help while the maintenance was done by the vendor.

Cost was not a driver.

In contrast, the big take off in 'cloud' happened with the CFOs getting convinced about the 'huge' cost savings, by shifting from capex to opex model and having the flexibility to invest only when required. After some initial resistance (to change, as always), CIOs also saw the inherent benefit that it provided them – by freeing them from a lot of nuts-and-bolts work.

Since, 70% of the costs went to the infrastructure technologies—like data centers—that is where both CFOs and CIOs focused. And the result was a huge take-off in cloud infrastructure services.

According to estimates by specialized research firm, Synergy Research Group, the annual spending on cloud infrastructure services went up from virtually zero in 2010 to an estimated USD 97 billion in 2019 (based on actuals of the first three quarters and estimates of fourth quarter). In the process, it overtook the spending on datacentre hardware and software, including servers, storage, networking, security and associated software, which is estimated to be worth USD 93 billion in 2019.

So, cloud infrastructure most unambiguously replaced captive data centers as the primary go-to infrastructure for enterprises.

Let's look at SaaS.

The same Synergy Research Group's estimates show that annual SaaS revenues in 2019 are expected to touch USD 101 billion. That is a growth of 39% year over year.

That is impressive, by any standard. Yet, in contrast to more than 50% share by cloud in the infrastructure area, SaaS accounts for just 23% of the total enterprise software sales, which stands at USD 445 billion globally. This means on-premise software still accounts for 77% of the total software that enterprises buy.

SaaS accounts for just 23% of the total enterprise software sales, which stands at USD 445 billion globally

A realistic assessment

What are the reasons why SaaS has not made a bigger shift?

A simple one line answer is: The shift is far more complicated.

According to Synergy, ERP, one of the biggest investment areas in software, is still, by and large, on premise. Even though ERP vendors have announced their SaaS versions, the change is not smooth. It is a different project altogether, and not really an upgrade. And what a project it is—with too many unknowns and uncertainties.

Since ERP is what keeps the business running, few are willing to take that kind of risk in shifting to SaaS.

Similarly, most vertical-specific operational support systems—the software that make businesses run—have also not shifted to SaaS.

This explains why despite impressive growths, SaaS has still not become the primary enterprise software model.

However, software like collaboration application and CRM have seen significant shifts to SaaS. Microsoft Office applications have seen significant shift to its SaaS-based Office 365 offering.

If we look at impact—and the buzz that some SaaS companies are creating—SaaS is very much the in-thing.

Consider this. More than half of the most impactful enterprise technology (hardware, software, services) companies in the last decade (2010-2019) were SaaS solution providers.

Among them are enterprise software development and collaboration platform Atlassian, electronic signature company DocuSign, communication and collaboration provider RingCentral, IT services management platform ServiceNow, ecommerce platform Shopify, cloud ERP vendor Workday, pharma industry software platform Veeva, and customer experience management platform Zendesk.

Six of these companies also find a place in Synergy's list of 12 technology companies that reached a run rate of USD 1 billion or more in the last decade.

Except for Workday, they are all specialized software firms.

It clearly shows that SaaS is on fire but the growth is being led by specialized solution providers.

In software, the change is typically upgrade; refresh is not as common and cyclical as in hardware. So, the change is comparatively slow.

Also, the initial model of SaaS getting entry into the enterprise through business routes—bypassing the CIO's office—has also got minimalized. While there is more involvement of business executives in the decision making today, both sides have walked some distance to find a common middle point. The decision making is more collaborative, and very little purchase happens bypassing the IT department completely.

This is visible in the marketing strategy of many specialized software firms. Tableau, which has now been acquired by Salesforce, was one of the super success stories of visual analytics, selling through the functional units route. But well before acquisition, it had changed gear and had started wooing the CIOs.

All these changes do take time. And so will the shift to SaaS.

In short, it is a matter of time — A when, not an if. ■

A Synapse To Deep Learning

The field of Deep Learning is an emerging field of Artificial Intelligence where machines synthetically break up data into metadata to enrich machine intelligence. Machines can learn by experience and acquire skills without human involvement

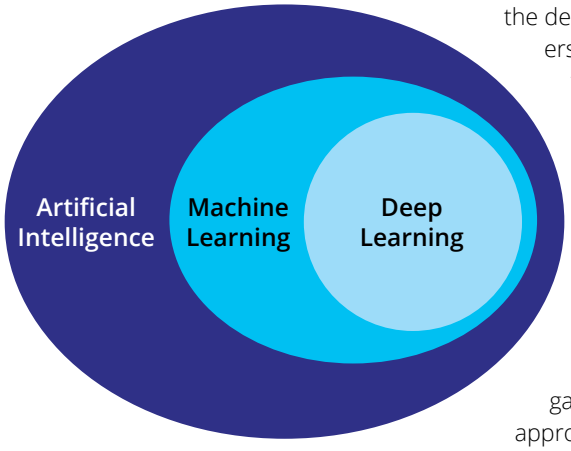
By PM Dutta

Machines are at the threshold of the digital era perfected to a crest of precision wherein only robo's can match or even excel the very perfect human results we rely upon today. Deep learning invokes machines to solve intricate problems even using a data set that is very diverse, unstructured and arbitrarily linked. The more deep learning algorithms built up data repository (intelligence), the analytics sharpen upon these diversified data using the layered learning mechanism, simulating a human brain's natural neural network(s). Neural data is filtered and converted into a nth-dimension tabular representation by extracting required attributes (metadata using common statistical metrics like mean/median, standard deviation, percentile, skewness, kurtosis, etc.) and then as an input to the next layer of filtering – a traditional machine learning mechanism.

The field of Artificial Intelligence (AI) is essentially where machines can do tasks that typically require human intelligence over neurons. It encompasses machine learning, where machines can learn by experience and acquire skills without human involvement. Deep Learning is a subset of machine learning wherein artificial neural networks, algorithms inspired by the human brain learning mechanism, learn from synthetically breaking up into metadata of large data bubbles. This data is unstructured and so diversified and huge by its nature that it takes years to manually comprehend and extract learning information. The incredible precision in deciphering the crux of information's augmenting to AI that uses fuzzy algorithm to perform recursively, each time tweaking it to a layer to improve the finesse. Deep learning extensively harnesses neural network/s structure of the similar organic neurons carrying impulses inside a human brain to respond to this stimulus and return the action to taken. Neural networks has various layers of logical data filtration that enable

learning about a problem that requires "a series of logical analytic thought", converging to a conclusion in solving problem/s. A basic logic to Deep Learning techniques is common deep learning algorithms over Convolutional Neural Networks (CNN), deep Q networks and recurrent neural networks.

Deep Learning simulation initiates the need for multi terabytes of crude domain data sets to filter over CNN with millions of micro dimensions in the data to synchronize to the data domain. The neural networks are designed to operate on image data, sensor data, and time-frequency calculation on spectrogram of a signal. Recurrent neural networks as LSTM (Long Short-Term Memory) networks that are designed to operate on sequential data of text and signals.



Deep Learning is a subset of Machine Learning, a second level subset of AI and a second level subset to Machine Learning over networks – capable of learning unsupervised convoluted data that is unstructured and unlabelled. Embedded algorithms with decision tree support vector machines over neural networks and ensemble methods are also known as deep neural learning or deep neural network. Learning algorithms harness high parallel computational Graphics Processing Unit (GPU) with capability to cognitive learning to these models. Of late, clustered servers on the cloud architecture seems to be a Capex savior.

The infinite petabyte volume of datasets generated at each quanta of time is incredibly staggering—currently estimated at 2.6 quintillion bytes/day—this resource skews up to the meadows of Deep Learning.

According to Leon A. Gatys from the Center for Integrative Neuroscience, University of Tu¨bingen, Germany, Convolutional Neural Network (CNN) Image representations are below:

Deep Learning algorithms are trained to create patterns from all transactions but also probe for patterns, signalling to alert for a fraudulent investigation. The final layer relays a signal to algorithms (handler routines) that may freeze the user's account until all pending investigations are finalized. While there will be multiple simulations, the above augments in decision-making and the design processes of designers in Machine Learning are focussed to Deep Learning. By understanding the differences between Machine Learning and Deep Learning, knowing the end application of a project and factoring in data and computing engine, design teams will gain faster insight into which approach fits best for their respective projects.

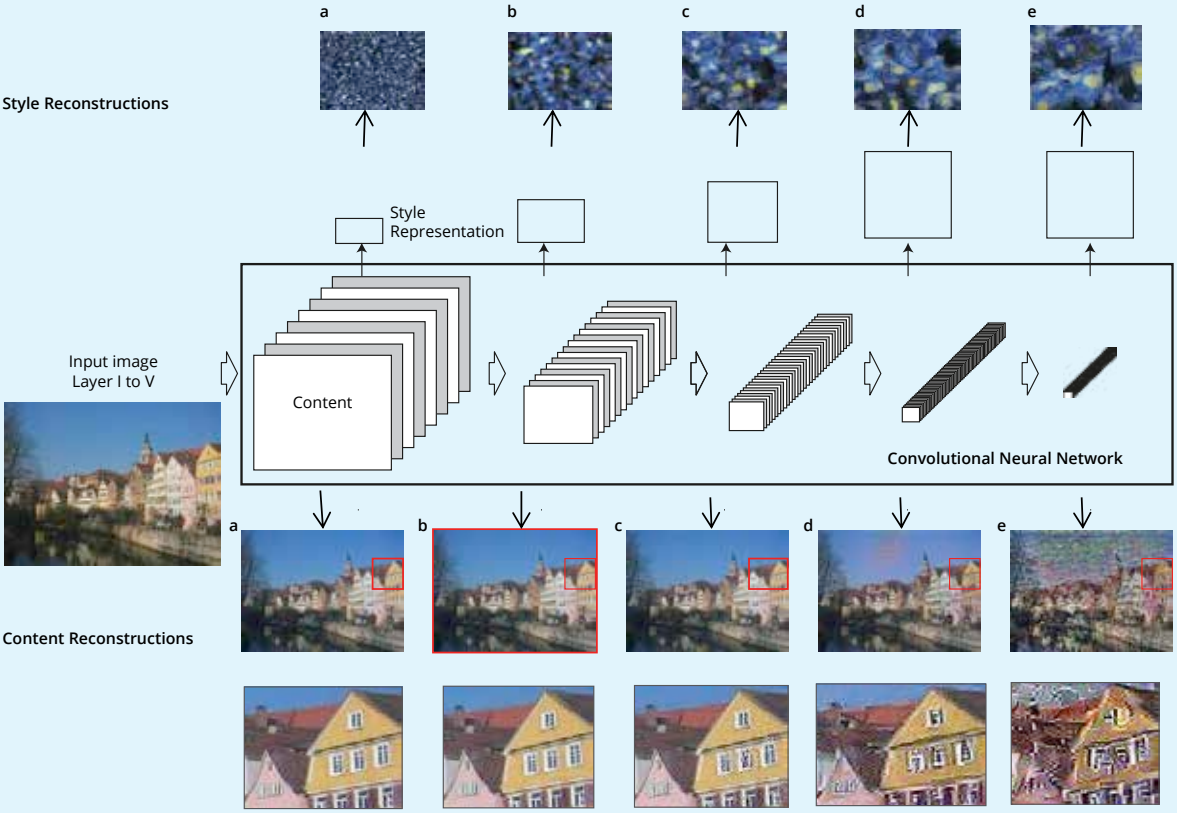
Deep Learning-as-a-Service (DLaaS)

Detection of fraudulent activities invokes profound Machine Learning. The data gathered goes to create a Deep Learning. The Machine Learning system creates a model with parameters built around the specific engines of the Deep Learning method(s), which starts building upon the repository as a prototype to infuse a hardening to Machine Learning algorithm. Deep Learning is used across all industries for a number of different tasks which has big data in commercial apps that use image recognition, open source platforms with consumer recommendation apps and medical research tools that explore the possibility of reusing drugs for considering the accuracy of automated approaches that are typically compared to the stringent standards of flawless human outputs. In reality it is accurate to the variety of tasks considered for AI/AR (augmented reality) automation, for example driverless car, real-time speech transcription tasks like creating closed captioning in TV news, Google's Speech-to-Text analytic API to name a few. It transpires that broadcasting systems are almost accurate in speech renditions of the voice delivery. The captioning of some broadcasting station's quality to the manual captioning can vary from day-to-day and even over the course of a day's time slice. The difference can be significantly measurable. Real-time transcriptions are typically outsourced to perform the data entry. Quality differs dramatically between contractors erstwhile the same individual might perform better in the morning when they are more rested than fatigued.

Different transcriptionists can show different kinds of errors, meaning the same word can be spelt correctly for part of the day and exhibit far more typographical errors during the rest of the day. In brief, humans are imperfect and the various people involved in the creation of real-time television can lead to a highly variable transcription error rate.

In contrast to automated speech phonetics (nowadays as cosmetics), transformation-to-text systems have a near-to-perfect consistency. The same tool/s executes the same video, again and again, with result of same output each time. That output may have errors/deviations in it, but those errors will be the same during each time of replay. Error consistency shows up as mis-spells to be fixed by adding the corrective spelling from the tool's custom dictionary. The accuracy of deep learning systems is a theoretical/utopian world over humans performing perfectly in an infinite domain of time. In reality, humans are imperfect and

Figure: Image representations in layers in a Convolutional Neural Network



(Source: Leon A. Gatys from the Center for Integrative Neuroscience, University of Tu¨bingen, Germany)

error-prone results with inconsistent accuracy deviate over the course of events at different time slices on the same day. Speech recognition is an area where humans at their best still typically outperform machines. In real-life, the real-time transcription tasks like generating closed captioning for television news turns out that commercially available systems like Google's Speech-to-Text API are actually almost as accurate as their human counterparts and are far more faithful in their renditions of what was said. Automation is closest to reality as machines at their ordinary can typically outperform humans at their ordinary to perfect consistency.

The surge to Deep Learning enriching the accuracy of automated approaches is typically compared to the gold standards of flawless human output. In reality, real-world human performance is actually quite poor

Automation is closest to reality as machines at their ordinary can typically outperform humans at their ordinary to perfect

at the kinds of tasks typically being considered for VR/AI automation. Cataloguing imagery, reviewing videos and transcribing are all tasks where humans have the potential for very high accuracy but in reality of their long repetitive mind crunching hours sitting in front of their workstations lose accuracy that depletes rapidly and varies dramatically from day-to-day and even hour-to-hour. By analyzing closely at the captioning of some transmitting stations, an interesting pattern emerges: The quality of the human captioning can vary from day-to-day and even over the course of a single day. Different transcriptionists can exhibit different kinds of errors. In this perspective, recursive number of machines can be launched to process an exigency situation, for example fire, quakes, flood, etc., of incoming content, with every instance performing precisely lossless presentation.

We can well conclude on the fact that by comparing machines against an idealized benchmark that simply doesn't exist, we should recognize that learning engines are increasingly reaching to a point where they can match or even exceed the very perfect human results we plinth upon today. ■

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

Navigating Tech-Clash A Key Challenge For C-Suite Leaders

Organizations must deliver more human-focused experiences, in line with what people have come to expect

By ITNEXT

Although there's been plenty of talk about 'tech-lash', or pushback against the latest technology, the reality is people are using technology more than ever. 52% of consumers say that technology plays a prominent role or is ingrained into almost all aspects of their day-to-day lives, according to Accenture's Technology Vision Consumer Survey. In fact, 19% report that technology is so intertwined with their lives that they view it as an extension of themselves. Globally, people spend an average of 6.4 hours online daily. They are post-digital.

Actually, instead of a 'tech-lash', it is a 'tech-clash'. People are not against technology; they remain excited and intrigued by it. But businesses are developing and deploying that technology using the playbooks of decades past, from the days before tech had such a major, meaningful impact in people's lives. Closed ecosystems can make experiences disjointed. Artificial Intelligence (AI) solutions are

applied to decision-making without transparency, leaving people out of the loop on decisions that directly affect their lives. Concerns about security, privacy and ethical issues keep people wary of companies' evolving digital technology innovations.

Navigating tech-clash is a key challenge for C-suite leaders in the next decade. Up until now, businesses have largely benefited from following the technology roadmap laid out by digital pioneers. Now, digital technology is evolving from an advantage to a basic expectation—and yesterday's best practices are turning into today's shortcomings. Therefore, organizations must deliver more human-focused experiences, in line with what people have come to expect.

Tech Trends

The new models that organizations must build to overcome 'tech-clash' share one thing: They are based on collaboration. Successful business leaders will invite customers, employees, partners and the public to build their new course for the future together. According to the survey, the following five tech trends exemplify this:

#1 The I in Experience

The traditional relationship between businesses and people is changing. Successful organizations are bringing a human focus to their digital interactions, designing a truly collaborative digital experience. This shift reflects a person's evolving expectations. It's clear that people want rich, customized digital experiences. But they have grown disillusioned by the legacy methods used by most organizations to deliver them. Models that served businesses well in the early days of the digital age have led them to inadvertently take more and more control away from individuals. Existing customization methods based on robust data gathering and analytics are failing to provide the transparency, or the agency, that consumers want. And it's not just customers. Cooperative digital experiences are also helping organizations re-imagine their partnerships with employees and other stakeholder groups.

Organizations that take the right actions today with cooperative digital experiences are setting themselves up for future success. As 5G and Augmented Reality (AR) become widespread, their significant impact on experience delivery will make balancing customization and user agency even more critical. Together, 5G and AR will enable businesses to tailor people's digital journeys throughout their lives, anywhere and anytime. With this omnipresence comes even greater responsibility to get it right; for the organizations that do, there will be huge opportunities.

Now, digital technology is evolving from an advantage to a basic expectation—and yesterday's best practices are turning into today's shortcomings

#2 AI & Me

Leaders have successfully adopted AI tools and practices that speed up the automation of basic tasks in existing workflows. But this is now table stakes. The true potential of AI in the enterprise lies in using it as a collaboration tool with humans: To not only efficiently execute tasks but also transform what businesses actually do.

It means smart chatbots interacting with customers as they do now, but being able to better understand the nuances and underlying possibilities of a customer's request. Meanwhile, based on the information the chatbot can gather, human agents are better prepared to offer assistance and improve the experience.

Hence, effective communication is the key. Because of advancements in Natural Language Processing (NLP), machines are beginning to better understand the context of language, instead of just the content.

Understanding physical context is also game-changing for AI's ability to work with humans in Extended Reality (XR) environments. Image recognition and machine learning allow AI to not just see its surroundings, but understand them.

It goes the other way as well, with humans being better able to understand machines. Explainable AI allows people to open up previously "black-box" AI systems to get at how the machine made a particular decision.

Ultimately, better human machine interactions will lead to businesses being able to reinvent and constantly improve the offerings and experiences their customers want. When steps are taken to improve communication between machines and humans, the result is that AI becomes much more than just another tech tool. It's an agent of change in the business.

#3 The Dilemma of Smart Things

In the digital era, everything is connected. The Internet of Things (IoT) market is expected to grow to 75.44 billion connected devices by 2025, with a projected market value of USD 1.1 trillion by 2026.

To unlock the full value of this opportunity, businesses need to confront the "beta burden," and the unintended consequences that occur when smart tech – smart products, and the experiences they contain – are constantly in flux. Organizations can now change the functionality of smart products or reconfigure their ecosystem over time. But they have to ensure that the customer experience remains consistent and supported throughout all these changes. Customers expect nothing less.

The upside of "forever beta" products is clear: Organizations that can respond to changing customer demands and expectations in real-time become true partners. The value of the product then grows. But in the flurry of constant updates and changes, customers can get left behind and frustrated. Organizations must update their understanding of what product ownership means in the post-digital era and change their practices as a result.

Organizations can overcome the "beta burden" by applying more flexible processes and Application Programming Interfaces (APIs). To overcome the beta burden, they will have to bring this mindset into every aspect of the enterprise, from sales, to customer support, development, design and more.

Doing so will help retain customer loyalty going forward by ensuring smooth transitions from one generation of smart products to the next.

Organizations can overcome the "beta burden" by applying more flexible processes and Application Programming Interfaces (APIs)

#4 Robots in the Wild

Organizations have already realized the benefits of robotics in controlled spaces, from lower production costs to higher productivity and increased capacity for analytics. Now, businesses are looking at the next frontier for robot technology: The open world.

Advances in sensors, speech recognition and computer vision are combining with lower hardware costs to make robot technology more accessible for organizations in every industry, and the rollout of 5G networks is set to unlock new opportunities outside of controlled environments. But finding the right way to introduce robots into the world includes challenges around talent, questions of human-computer interaction and a test-bed that consists of the entire world.

A massive robotic migration will demand a combined approach to development and testing. Experimentation will be the key as technology is introduced to city streets, university campuses, construction sites, and other uncontrolled environments. It will also require a commitment to continuous data collection and refinement after the devices have been deployed.

#5 Innovation DNA

An organization's innovation DNA is made up of three building blocks: Maturing digital technology that is more commoditized and accessible; scientific advancements that push the boundaries of industries and inspire change; and emerging DARQ (Distributed Ledgers, AI, Extended Reality and Quantum Computing) technologies that are poised to scale rapidly. Where organizations differ however, is that they can cultivate their DNA to drive business transformation.

Today, leaders are weaving these technological building blocks together to set a course for their organization's future. For businesses, the path forward begins with a renewed focus on technology transformation as they find their unique combination of building blocks and develop their innovation DNA.

It all starts by understanding the innovative business solutions that each building block provides.

Maturing digital technology is no longer just an advantage — it's a requirement. Many companies are finding new value by putting a price tag on their capabilities while also making them more accessible to those within their ecosystem.

Meanwhile, advancements in science are helping organizations expand beyond the digital world. From material sciences to genomic editing, organizations are turning these disruptions into competitive advantages faster than ever before.

Finally, organizations are finding new ways to inject DARQ technologies into mature markets. This is helping to ground these tech explorations in reality and open up doors to innovative business solutions.

While not every business will have each of these areas fully developed, it's important that they remain open to each of them as they build their own innovation DNA. Organizations can reap huge benefits by combining these different innovation building blocks. Moreover, leaders will align seemingly separate innovation strategies to radically differentiate themselves, leapfrog industry competitors, build a new generation of products and services, and even create new markets. ■

Double Scoop

Two times the revelation

Chetan Shah

Head - IT, L&T Technology Services

MY FAVORITE MOVIE

A Wednesday

MY FAVORITE CAR

Audi

MY FAVORITE SPORT

Cricket

AN EMERGING TECH THAT'LL CREATE HUGE IMPACT IN 2020

Cloud Security

A TECH SHOW I LOVE WATCHING

BizTech CES 2019 on YouTube

MY PEER IN THE IT COMMUNITY

Vibha Naik, Head - IT, Linde Engineering India

Vibha Naik

Head - IT, Linde Engineering India

MY FAVORITE GETAWAY

Mahabaleshwar

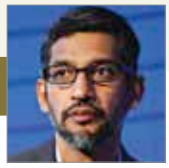
MY FAVORITE SINGER

Lata Mangeshkar

A TECH GADGET I USE FREQUENTLY

Smartphone

A TECH GURU I ADMIRE



Sundar Pichai

MY FAVORITE COLOR

Green

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

facebook.com/digitgeek

digit.in/facebook

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

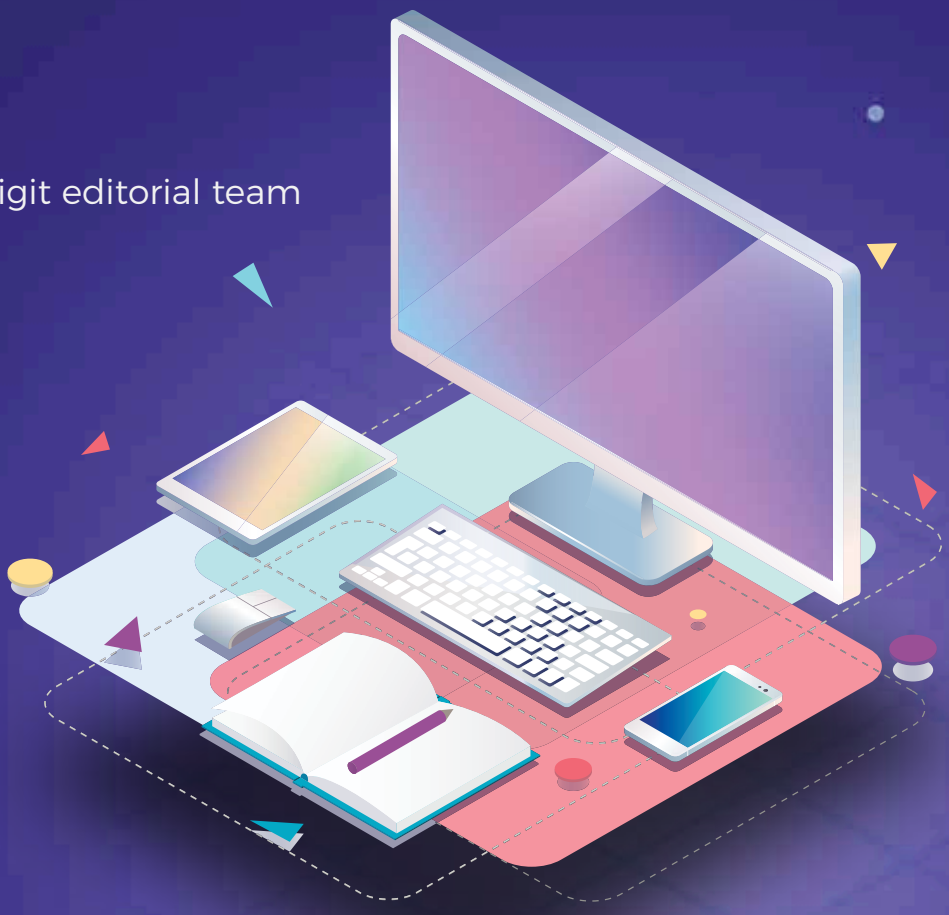
LAUNCHING

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

DELL Technologies

OPTIPLEX 7070 ULTRA

The desktop you didn't expect.

The OptiPlex 7070 Ultra is the world's most compatible, fully modular zero footprint desktop solution.* Its discreet design features swappable elements for ultimate flexibility and performance.

SMS OPTI to 56263 | 733 860 7474 | DELLTECHNOLOGIES.COM/OPTIPLEX

Windows 10

The best devices in the world run Windows 10 Pro.

*Based on Dell internal analysis of competitive products, June 2019. Ultra 7070 supports Dell and 3rd Party VESA Displays up to 27" (68.58 cm), sold separately. Zero footprint solution requires OptiPlex 7070 Ultra Fixed or Height Adjustable Stand, supporting VESA mounted displays up to 24" (60.96 cm) and 27" (68.58 cm) respectively.