Opinion | Pg 12
GDPR - A Turnaround For Marketers?

Feature | Pg 35
Why The New Digital Communication Policy Should Matter To IT Leaders?

IT NEXT
FOR THE NEXT GENERATION OF CIOs

How are Indian Security Leaders Preparing for GDPR?

15 security leaders reveal what they are doing to comply with European General Data Protection Regulations...

June 2018 | ₹100 | Volume 08 | Issue 13 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

DON'T GAMBLE, BE PRACTICAL

Join us at

19th CIO&LEADER CONFERENCE

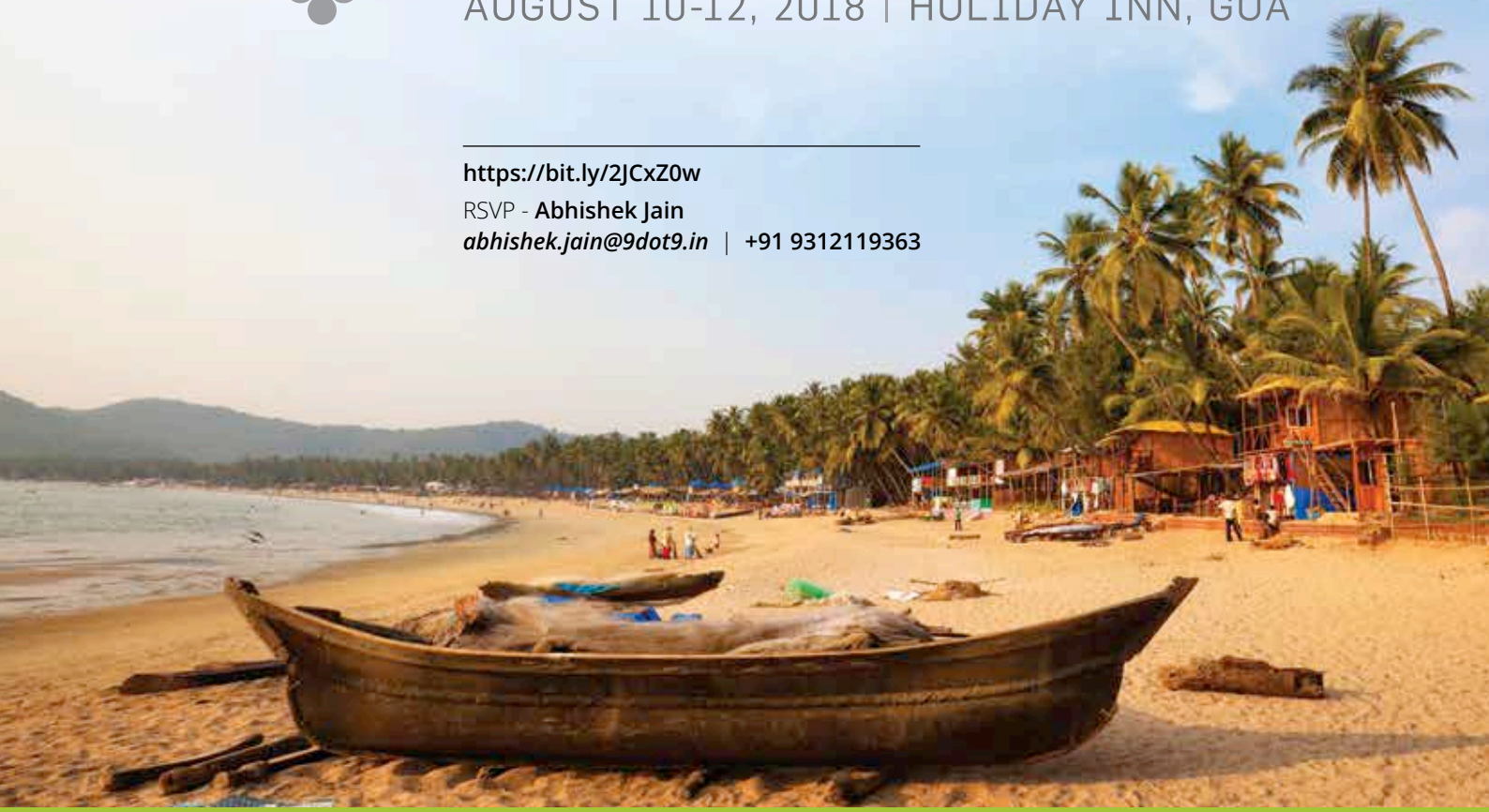
THE PRACTICAL CIO

AUGUST 10-12, 2018 | HOLIDAY INN, GOA

https://bit.ly/2JCxZ0w

RSVP - **Abhishek Jain**

abhishek.jain@9dot9.in | **+91 9312119363**



#thepracticalcio #cioannual

GDPR as a Bellwether of the New Age of Privacy

GDPR reminded businesses going overboard on opportunities of collecting and analyzing individuals' data that it is a party that they must pay for—by complying to a set of rules about what they can do and not do with what personal data of individuals, apart from keeping that in safe custody.

Shyamanuja Das

How are Indian companies preparing for GDPR?

That is too hopeful a headline on the cover.

Never mind that less than 20% Indian companies have to do anything about GDPR. The 15 odd security leaders whose comments—very few of them plans—about GDPR have been featured in this issue belong to that 20%. We have, for obvious reasons, not included those who said it does not apply to them.

It would not have been such a big thing without India's quasi-global technology and business services industry, commonly known as IT/BPO. However, we do not feature it here because of them.

GDPR is a big word for all. It is a big word because it reminded businesses going overboard on opportunities of collecting and analyzing individuals' data that it is a party that they must pay for—by complying to a set of rules about what they can do and not do with what personal data of individuals, apart from keeping that in safe custody.

By enacting a very stringent piece of regulation, it showed the world that if you have strong will, you can actually do it, despite all criticism.

It is a piece of regulations that showed the path to governments worldwide on what to do about protecting its citizens' privacy. That many of the global policy considerations—including those discussed by the white paper made by an Indian committee entrusted with proposing the provisions of a proposed data protection law—are based on GDPR is not a coincidence.

Despite all that, the sensitivity about individual privacy is still very low in India. Part of the reason is Indians themselves care very little about privacy. Give a recharge of ten rupees and many are willing to share everything. In an environment like that, making a stringent data protection regulation work is a tall order.

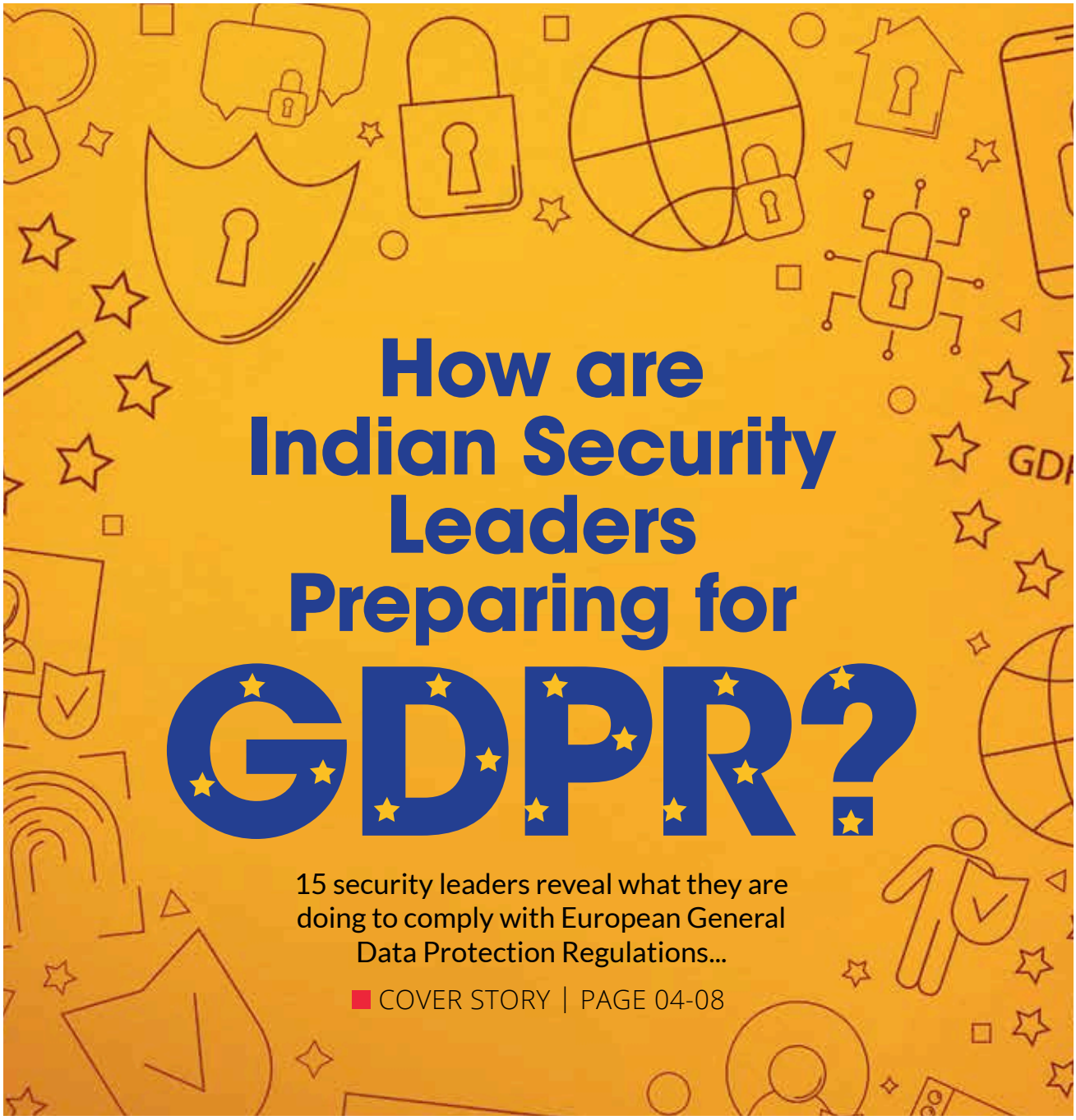
But GDPR has begun on a right note. I doubt if there would be large scale penalization in the first few months. But as the regulators there have shown, they have strong will and they will not hesitate to take action. And penalties like 4% global revenue are not a matter of joke.

If they can do that successfully, other governments will follow suit.

CISOs have of late become CCOs—Chief Compliance Officers. This challenging task of complying with these regulations will be on them. The journey has just begun.

JUNE 2018
VOLUME 08 | ISSUE 13

Content



How are Indian Security Leaders Preparing for GDPR?

15 security leaders reveal what they are doing to comply with European General Data Protection Regulations...

COVER STORY | PAGE 04-08

OPINION | PAGE 12
GDPR - A Turnaround For Marketers?

OPINION | PAGE 13
IoT Sensors In Agriculture

INSIGHT | PAGE 18-19
Maximizing Gains By Combining New Digital Investments

INSIGHT | PAGE 26
India Public Cloud Revenue To Rise In 2018

FEATURE | PAGE 35-39
Why The New Digital Communication Policy Should Matter To IT Leaders?

COVER Design:
CHARU DWIVEDI

ADVERTISER INDEX

Schneider BC

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
Associate Editor: Shubhra Rishi
Content Executive-Enterprise Technology: Dipanjan Mitra

DESIGN
Sr. Art Director: Anil VK
Art Director: Shokeen Saifi
Visualisers: NV Baiju & Manoj Kumar VP
Lead UI/UX Designer: Shri Hari Tiwari
Sr. Designers: Charu Dwivedi, Haridas Balan

SALES & MARKETING
Director-Community Engagement: Mahantesh Godi (+91 9880436623)
Brand Head: Vandana Chauhan (+91 99589 84581)
Assistant Product Manager-Digital: Manan Mushtaq
Community Manager-B2B Tech: Megha Bhardwaj
Community Manager-B2B Tech: Renuka Deopa
Associate-Enterprise Technology: Abhishek Jain

Regional Sales Managers
South: BN Raghavendra (+91 9845381683)
North: Deepak Sharma (+91 9811791110)
West: Prashant Amin (+91 9820575282)

Ad co-ordination/Scheduling: Kishan Singh

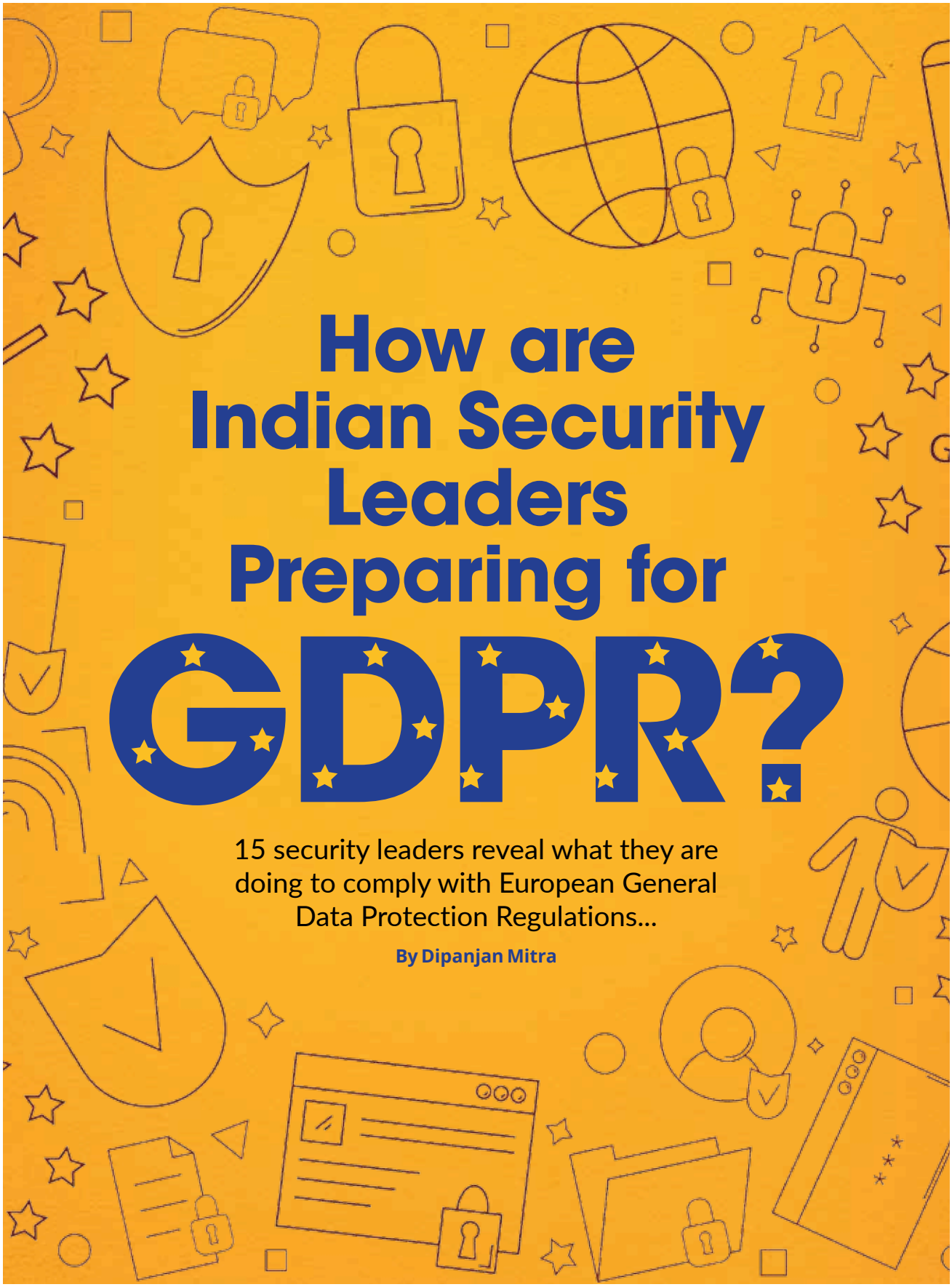
Manager - Events: Naveen Kumar
Manager - Events: Himanshu Kumar

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

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



How are Indian Security Leaders Preparing for GDPR?

15 security leaders reveal what they are doing to comply with European General Data Protection Regulations...

By Dipanjan Mitra

May 25, 2018. It was like any other summer day. Except that for thousands of senior IT and security leaders globally—whose organizations do business in Europe or have anything to do with any personal data of European citizens—it marked a day that would change their lives for ever.

The day came and went. We have no way of knowing how prepared the organizations are, except, of course, those that have announced their programs publicly.

GE, for example, has developed a GDPR framework to facilitate its implementation. Bosch has clearly outlined its data protection policy since the GDPR came into effect. So has Philips and a few others.

Most of the European companies would surely have done something to ensure that their customer data is protected as flawlessly as possible. A single breach can make you pay 4% of your annual global revenue.

The regulations apply to any company that handles personal data of European citizens.

In, India, GDPR is big news because of two reasons. One, there's a whole industry here that is built on providing technology and business services to companies everywhere, Europe being the second largest market after the US. Two, these are the guys (the IT companies) that are helping the European companies in being compliant. That way, it is an opportunity and challenge at the same time.

It must be mentioned here that GDPR does not apply to UK—the European country that India does most business

"GDPR has certainly upped our level of controls and made us deep-dive into where sensitive and personal data lies. It is helping us understand where the data is flowing. GDPR is bringing a proper method in place because cyber security, privacy and all such concerns are increasing by the hour. Being from the security industry, we want people to be comfortable using products and services and ensure that their data and security is being taken care of. So GDPR is a very welcome move and is positively impacting our business."

Anuj Tiwari
CISO, HCL Technologies

INDIAN SECURITY LEADERS ON GDPR

"We have 3-4 entities which have come under GDPR and have appointed a local consultant too, who is taking care of total compliance of law."

Sanjeev Lamba
Head IT GRC, Uno Minda Group

"Since we are dealing with NRI customers, GDPR applies to us too. We have contacted our legal team to find out how it can be enforced along with third-party vendors who will also be under the ambit of GDPR."

Vinod Negi
Senior Chief Manager – Information Security & Risk, Dewan Housing Finance Corp

"We've evaluated the controls within GDPR, did analysis and have taken action to comply with GDPR."

Kishan Kendre
Senior Manager, Reliance Industries

"There are expectations to abide by the regulations. Companies are preparing to follow the controls which are in place."

Aashish Narkar
Global Head – IT Security (Internal IS), TCS

"GDPR should not be done just for compliance purpose but should be maintained for the benefit for our data. At ABP, we follow ISO norms as practice and similarly, GDPR needs to be followed by every organization as practice."

Subhanil Banerjee
Senior Manager – IT Infrastructure & Security, ABP

"With the effect of GDPR, we have brought down a few of our services from the website. For example, we have stopped our biometric services and replaced it with smart cards."

Satish Asnani
Deputy General Manager, BHEL

with; but it has its own data protection rules, almost as stringent as GDPR.

So, how are Indian companies doing as far as complying with GDPR goes? We decided to ask the security leaders themselves.

And guess what—we asked them on 25th of May, the day GDPR was kicking in.

The answers were not too surprising. Most companies

"We have incorporated data leakage prevention tools in our infrastructure as well as threat detection tools which help in threat landscaping. GDPR will be a big boost to the security landscape."

Aditya Khullar
Technical Leader – Security, One97 Communications

"We are a global company and data security and privacy is our key practice area. We have to now align GDPR to our internal data, client data and ensure it is placed on our global location."

Sandip Sannyasi
Consultant – Cyber Security, Dell Technologies

"In terms of GDPR, we are looking at classifying data, ways in which we can protect our users, and who will be really impacted. So we are trying to identify these areas."

Vaibhav Pendurkar
Head – Information Security, FIS Global

"If organizations can measure upto the compliance levels of GDPR policy, then it will hold them in good stead. Many organizations have already started working on it."

Rupen Shah
Assistant General Manager – IT, Arohan Financial Services

"GDPR will help organizations to have better managed infrastructure, better communication outside the organization and will create an ecosystem where every stakeholder will be safe, secure and use the entire set-up in a safer way."

Sunil Pandey
Director – IT, Institute of Technology & Science

"For us, the impact of GDPR is huge. We are working with a team based out of France to ensure that we are identifying all data points where personal data is getting stored and processed. We are implementing all possible controls to ensure 100% compliance."

Shweta Nair
Senior Manager, Capgemini

who had to comply have started in right earnest; there's no other way. But as with a new initiative, people described action—what they are doing—rather than what they have achieved.

As expected, IT/BPO companies are ahead of the curve.

"Since, we were already certified in ISO 27001, SOX and SSAE 18, it was easy to implement all the GDPR controls. Also, as we are a HIPAA company, HIPAA and DPA controls

"In terms of GDPR, we had to ensure putting all our policies and procedures in place and updated all our documents and are in compliance to its requirements. The laws are very stringent and you can be fines billions of Euros in cases of non-compliance. Since, we were already certified in ISO 27001, SOX and SSAE 18, it was easy to implement all the GDPR controls. Also, as we are a HIPAA company, HIPAA and DPA controls were also configured along with the 27001 controls. So we were already compliant with the UK Data Protection Act. Thus, GDPR compliance was a bit easy and we have also been able to convince our customers that we are complying with those requirements."

Rajiv Nandwani,
Director & VP, Global Information Security, Innodata

were also configured along with the 27001 controls. So we were already compliant with the UK Data Protection Act," says Rajiv Nandwani, Director & VP, Global InfoSecurity, Innodata. GDPR compliance was, hence, a bit easier.

While IT/BPO companies GDPR as a high priority, some of the other companies are learning that they have to comply as well. Take Dewan Housing Finance, a housing finance company in India. Why are they worried about GDPR?

"Since we are dealing with NRI customers," says Vinod Negi, Senior Chief Manager – Information Security & Risk, "we have to be compliant".

"We have been speaking to our legal team and figuring out how it can be enforced and also contacting with third-party vendors who will also be under the ambit of GDPR," he adds.

In India, however, 7 out of 10 BFSI organizations (handling EU customer data/business) we reached out to did not want to comment on their GDPR preparedness. However, all of them had heard of the regulation and its impact of their business, unlike a quarter (25%) of the 700 European companies surveyed by IDC Research on behalf of ESET, admitted they were not aware of GDPR and more than half (52%) of them were unsure of the impact on their organizations.

Research firm Gartner, in a statement issued in November 2017 believes that less than 50% of all organizations impacted will fully comply by that date.

The IT/ITeS sector is the biggest contributor to India's economy – with 66.1% contribution of services sector to GDP, the information technology – business process management (IT-BPM) sector serves as a major market for IT software and services exports are the US and the UK and Europe, accounting for about 90% of total IT/ITeS exports. Given the criticality of IT–BMP services, "India must do all it can to protect and promote business in this sector. To a large extent, future of business will depend on how well India responds to the changing regulatory changes unfolding globally. India will have to assess her preparedness and make convincing changes to retain the status as a dependable processing destination," - according to a white paper, titled GDPR and India, written by Aditi Chaturvedi for The Centre for Internet and Society.

"Even though GDPR has come into effect, we are not in haste. We have basic disciplines in place and will take steps to see what are the plug-ins we have to make and will be able to manage it accordingly. "

Durga Prasad Dube
Senior Vice President, Group CISO & Head – IRM, Reliance Industries

For Indian companies that have to comply with GDPR, it may come as a blessing. India itself is in the process of enacting a stringent data protection law. A committee was formed by the Government of India for working this out; it has already released its discussion paper listing important issues and has got public inputs. A draft policy should follow.

With Supreme Court of India's landmark verdict on the right to privacy, it is a matter of time before India moves to the new data protection regime. Those who have complied with GDPR should find it much easier to comply with those requirements. ■

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

EXTRA Curricular

Aniruddha Mehta playing the Harmonium and Guitar

Sing Along

NEXT100 Winner 2017 **Aniruddha Mehta**, Head – Quality Informatics, Alembic Pharmaceuticals shares his intense passion for singing. Besides, he also takes a keen interest in photography (landscapes).

"Music touches us emotionally, where words alone can't."
– Johnny Depp

"Music in itself is healing. It's an explosive expression of humanity. It's something we are all touched by. No matter what culture we're from, everyone loves music."
– Billy Joel

My fascination and love for music started as a kid with the LP discs and player, which my father had and I still possess. This introduced me to some amazing genres, such as Jazz, Western Classical, Indian Classical and OSTs. Moreover, this gave me an insight into singing styles and an introduction to various musical instruments. I became so obsessed that my day started with music and ended with music.

I grew up listening to legendary singers like Kishore Kumar, Mohammad Rafi and Yanni and Pandit Jasraj. Kishore-da's amazing composition of 'Koi Humdum Na Raha' and Mohammad Rafi's 'Azaan' stands out for me. Also, I fondly remember Pandit Yasraj singing "Govind Damodar Madhaveti" live in a school in Gujarat as well as Yanni's famous concert at the Taj Mahal in Agra, which was noth-

Aniruddha Mehta *Snapshot*

Aniruddha Mehta is Head - Quality Informatics at Alembic Pharmaceuticals. He is a winner of NEXT100 Award in 2017. He has done his Bachelors in Engineering & Technology. He has also worked in managerial positions at Cipla and NSDL and software engineer at Infosys.

ing short of magic. Yanni's ethereal keyboard work backed by an orchestra, vocalists, a choir, and various world instruments including didgeridoo, duduk, charango, and bamboo saxophone still reverberate in my ears.

This inspired me to learn Indian classical music and at the age of 7, I was blessed to receive my first music lesson from the Late Gainyji (Father of music director, Uttam Singh). I not only learnt to play the keyboard but also the harmonium, table, bongo and violin. I made maximum usage of these instruments during my participation in intercollegiate competitions and events.

I also listen to noted singers like A R Rahman, Madan Mohan, Madonna, Billy Joel, Frank Sinatra, Amit Trivedi, Anouska Shankar, Arijit Singh, Sonu Nigam, Jagjit Singh, Ghulam Ali, Enya, Eric Clapton, Hans Zimmer, Lionel Richie, Bach, Beethoven and Richard Clayderman. I've tried to not only play their songs in-house but also publicly. Even the musical instruments they play, I've tried to replicate them in my shows too.

So music for me is a combination of "Lay" (Tempo), "Sur" (Notes) and "Taal" (Rythm). It is not only an art but also science and the optimum combination of the above three tends to give you a sonorous melody. Like Mozart said, "Music is not in the notes, but in the silence between." It actually hasn't changed much except maybe the way it has been delivered. For instance, the way Rahul Sharma has taken Indian classical music to a completely different zone and created some beautiful collaboration with likes of Kenny G and Richard Clayderman.

Aniruddha Mehta on his Keyboard

In future, too, I want to remain inundated in music and keep up with my singing. I also hope we will continue to keep coming up with beautiful lyrics and tunes, which will create the magical and soulful song which we all crave for.

After all, what is a life if there is no music! It defines everything from happiness to sorrows to peace to joy. So keep listening, keep singing! ■

As told to Dipanjan Mitra, Team ITNEXT

GDPR - A Turnaround For Marketers?

Will we see a resurgence of campaigns like - Made for Each Other, Marlboro Man or for that matter Fosters - Australian for Beer?

By Prateek Chatterjee

I was chatting up with Jodie Sangster, CMO Liaison Lead, IBM Watson, post an impressive session by her on GDPR (General Data Protection Regulation) at the DMA Asia's Digital Breakfast briefing...something she said during her presentation got me thinking. She mentioned that GDPR is actually going against the grain of AI, whose very premise is data driven analytics. So I asked her later - does it mean that we may no longer have the luxury of data profiling...not even the types wherein we don't know the name but know the attributes, which can help trace the journey back to the profile...to that she mentioned, even data of these sorts will get increasingly hard to harvest and target, given the stringent data protection laws under the new GDPR regime, which kicked in from May 25th for EU.

That brought me to my follow through query. What about the psycho-graphic profiling that we do on Digital to hyper target a set kind of TG?...yeah, you got it - all that will change too.

So what happens to Martech...the hyped avataar of profiling and hyper targeting? Marketing communications of late has become an extension of Martech, which is led by data driven campaigns. Everything is now about profiling the right audience and reaching them with customized messaging. Creativity actually happens by accident. Brand communication takes a back seat in a Martech world.

Will GDPR then, be a whiff of fresh air, where the focus shifts back to storytelling, content and creativity...rather than overt reliance on tools, in the wake of hard to harvest data regime?

Will we see a resurgence of campaigns like - Made for each other, Marlboro Man or for that matter Fosters - Australian for Beer? Suddenly I see Jodie's eyes light up ! (she's Australian herself)...

While the jury is still out on this, so far it seems that GDPR may just be that manna that frees us from the shackles of Data slavery. Sentiments, Brand salience can once again occupy centrestage...meeting the unmet need (rather than giving people more of what we think they need) can once again usher new waves of innovation, like iPhone did for the entire communications sector.

Someone once said that a brand story is something that you feel between the ears. Am hoping that GDPR lets the fresh air in, so that we can breathe a little more deeply...and live a little more joyfully.■

The author is Senior Vice President, Corporate Communications & Marketing at NIIT Limited

IoT Sensors In Agriculture

The sensors we have today (whether video, hyperspectral or infrared) allow us to understand many of the conditions of plants in the field

By Adam Drobot

There's a common misconception that farms are simple places. While that's never particularly been the case, modern agriculture is impressively complex and technologically sophisticated, and is becoming more so with the introduction of a wide array of sensors.

The sensors we have today (whether video, hyperspectral or infrared) allow us to understand many of the conditions of plants in the field. The sensors can be based on different platforms, from satellites and high altitude aircraft to smaller drones that are flown and controlled locally, to permanent sensors mounted on structures that overlook the field. The data from these sensors is used to understand the spatially-resolved field conditions and how the crop is progressing. Interpreting sensor data and the spatial distribution can be used to determine how the field should be managed to achieve the best yields, and where and when to harvest the crops. In terms of plants, miniaturized integrated sensors that are low-cost and can be placed on individual plants is one direction we could see. It all depends on how the cost can be reduced enough to match the economics of farming.

Also, if we talk of the key technological advancements that would allow for the creation of cheap, miniature sensors, we need to mention the use of basic components from consumer electronics where large markets drive economies of scale. The best examples are cheap cameras that now cost a few dollars because of smartphone production volumes, accelerometers from MEMS technologies, and other developments that come from system-on-a-chip (SOC) design and manufacturing techniques. Satellites also play a huge role in assessing the condition of plants. Firstly, an increasing number of satellites use high resolution sensors – both optical and hyperspectral – to improve techniques for interpreting sounding data. There are also many more low Earth orbit (LOE) satellites, whose arrays provide much better coverage, both geographically and in field re-visit rates. The second role is as communications relays for ground sensors in sparsely-populated and under-resourced areas.

Drones also have great potential – they're just getting started. Because they can get right to where the action is, drones can be used to fly instruments that would not fit or work on satellites. An example is acoustic sensors used to identify pests and animals, data that's not possible to gather from satellites. A drone can also pick up a soil or plant sample that a satellite cannot.■

The author is IEEE senior member and Chair of the IEEE Internet of Things Activities Board

Building Better Data Protection And Steering Clear of GDPR Violations

Enforcement means that organizations should already be processing personal data in accordance with the GDPR — including provisions for data subject rights

By Nilesh Jain

The General Data Protection Regulation (GDPR), adopted in April 2016 after four years of deliberations, is now in force. The regulation made headlines around the globe with its stricter data protection standards, substantial fines, and most of all, extensive reach. The GDPR affects any organization that holds an EU citizen's personal data, no matter the size or location. A company based in Asia is as accountable as a multinational enterprise with offices across Europe — as long as it collects and processes the data of EU citizens.

The regulation also delineated the data protection obligations of affected organizations — from adopting state-of-the-art security methods to providing people more access to and control of their data. Recognizing the sweeping changes required for compliance, the EU authorities granted member

states and organizations two years to get ready and prepare. And today, the transition stage is over — the GDPR will now be enforced.

What happens now?

Enforcement means that organizations should already be processing personal data in accordance with the GDPR — including provisions for data subject rights. Data Protection Authorities (DPAs) of EU member states will also already be able to penalize organizations that are not compliant. Depending on the member state, it is possible that regulators will immediately take action to address any noncompliance. Some regulatory bodies, however, plan on being more lenient with businesses and organizations that have started but not yet completed their compliance efforts.

What is the worst-case scenario? An organization is liable for damages caused by noncompliance and is subject to corresponding administrative fines. The heftiest fine is 20,000,000 euros or up to 4% of annual turnover, whichever is higher.

What is the best-case scenario? If an organization is fully compliant with the GDPR, or uses the regulation as a starting-off point and goes beyond the minimum standards, then there are significant advantages. Some benefits would be: Secured valuable information, more efficient operations with proper archiving and data management, and increased trust from customers and users.

While the GDPR applies to personal data of EU citizens, the GDPR has sparked a change in privacy regulations across the world. The 2018 enforcement allowed several countries to make their own legislative improvements — the UK and Australia are just two of a number of regions that have also updated their data protection laws. This only indicates that GDPR compliance is a good opportunity — not just for multinational enterprises but smaller organizations as well — to keep up with global advances in data privacy and state-of-the-art security.

What should organizations be doing?

Ideally, all the groundwork for compliance should have been finished by now, and items on the compliance checklist should have been ticked. Organizations should already be able to provide products or services that address their customers' rights as outlined in the GDPR. Those using third-party applications or suppliers should watch for updates concerning issues like the "right to be forgotten" and stricter user consent standards and make sure they are working properly. Several laws as well as software changes are also expected to be in effect starting today or in the coming months, and organizations should be ready for any necessary changes.

For those not yet fully compliant, some member state DPAs have reassured companies "acting in good faith" or on the way to compliance that they will initially be treated with consideration. It's crucial to document steps being taken as well as to prioritize addressing potential security risks.

Ready or not, the road to GDPR compliance does not end on enforcement day — assessments and audits should be regular moving forward.

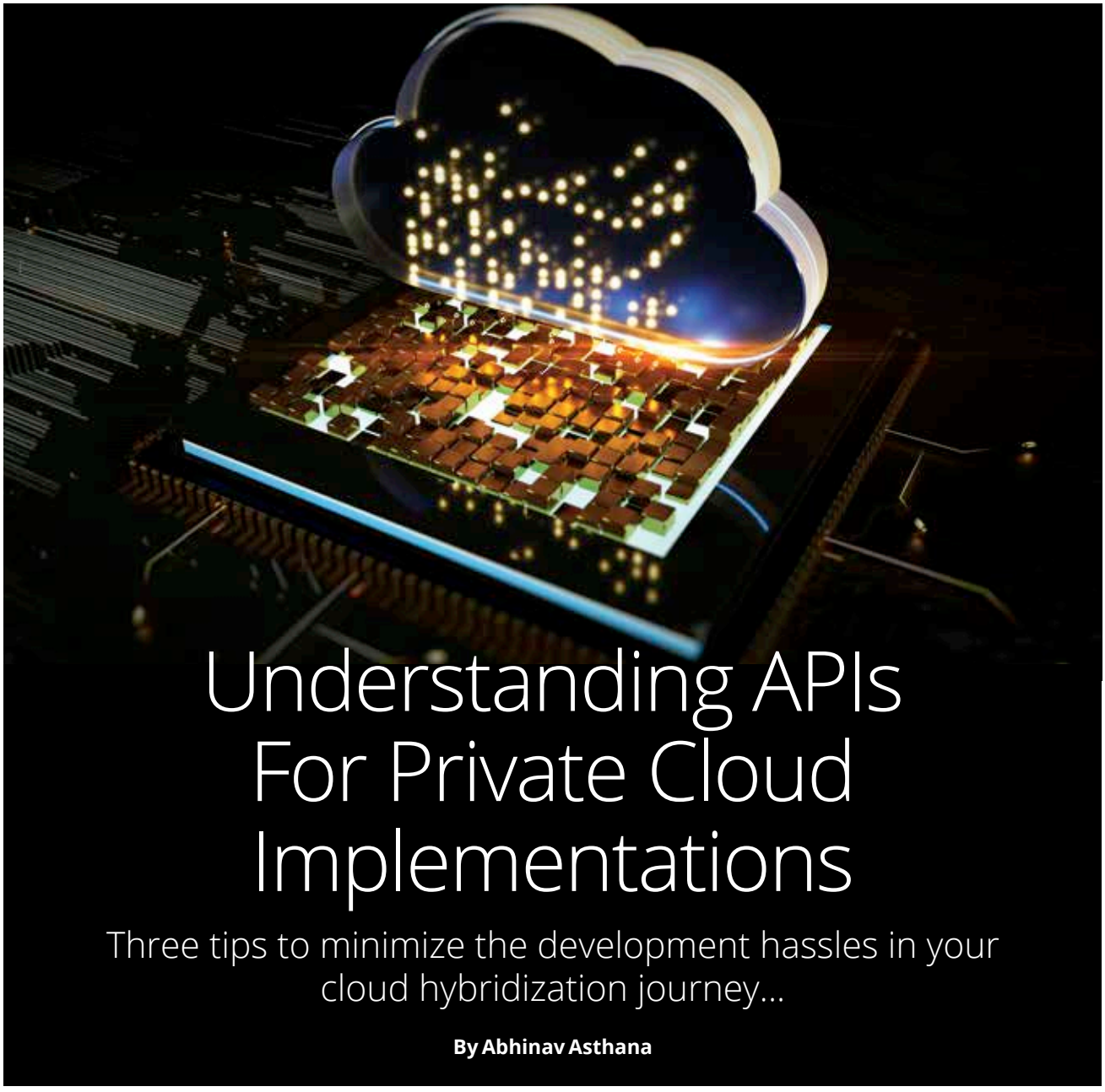
Through its new rules and standards, the GDPR encourages organizations to rethink existing data management policies and invest in state-of-the-art security for data protection.

Building better data protection

The GDPR was enforced to set a new standard for data privacy and protection. One key element to this is building in privacy measures from the first stages of development — not patching up problems after they occur. As organizations create new products and applications post-implementation day, privacy by design must be kept in mind.

Through its new rules and standards, the GDPR encourages organizations to rethink existing data management policies and invest in state-of-the-art security for data protection. To reiterate, compliance efforts should be constant after GDPR implementation day; staying up to date with cybersecurity developments plays a major part.■

The author is Vice President – South East Asia and India, Trend Micro



Understanding APIs For Private Cloud Implementations

Three tips to minimize the development hassles in your cloud hybridization journey...

By Abhinav Asthana

Given the ecosystem complexities of hybrid cloud deployments, API management can be tough.

While addressing Inspire Partner Conference in 2017, Microsoft CEO Satya Nadella made an interesting observation when he opined that in the fight between public and private cloud, it's the hybrid cloud that has emerged the winner. Nadella's statement gets validated when one views the rise of hybrid cloud as part of the overall cloud market. According to Markets and Markets, the global hybrid cloud market is forecast to be valued at USD 91.74 billion by 2021, growing by 22.5% CAGR. Compare this with the overall cloud computing revenues of USD162 billion in 2020 (growing from USD 67 billion in 2015).

A highly sought after model by CIOs, hybrid cloud offers organizations a flexibility to use cost-effective resources and innovative features from public cloud vendors as and when required while retaining the advantages of tight management controls that their private cloud deployments assure. The hybrid model, however, can be a challenge to the backend API developer who has to ensure that users can move from one model to another seamlessly without compromising on the organization's

security and compliance mandates. Let's explore three API management good practices companies may follow to get the best out of their API programs for hybrid cloud implementations.

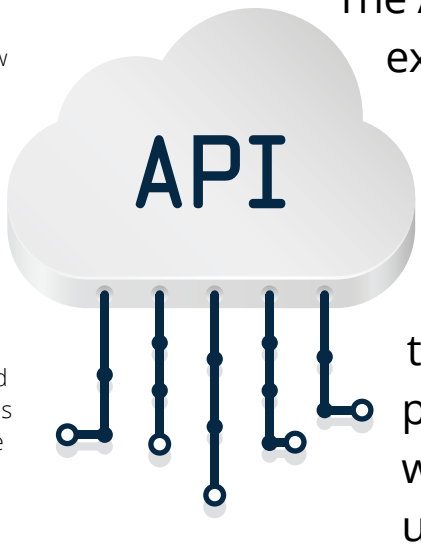
Streamline the database access needs of individual components

Generally, a hybrid cloud set-up presents a complex ecosystem of applications, business processes, and infrastructure components. Given this complex environment, when multiple components spread across business and application process flows are accessing database, it may impact performance of the whole system. In any case when components are moving into the cloud, performance gets affected further. An aspect to consider, here is the type of data–whether it is persistent or non-persistent.

The API management exercise should therefore, begin with mapping the database access needs of various application components with the linked business processes, and application workflows besides the user access levels. Ensuring that the database access function is carried out by one or only a few components may be a good approach to follow. Creating controlled interface(s) for public cloud-components to access applications and data from your private cloud may also be deemed useful.

Do not ignore security and support

In a hybrid cloud set-up APIs work as the pipe that provides access to enterprise resources to users—internal as well as external. Safeguarding sensitive business information is, therefore, an important task APIs must perform. A combination of security provisions including basic authentication via API keys, the advanced authorization model by using OAuth 2.0, and JSON Web Tokens (JWT) along with encryption may be considered a reasonable solution stack to secure API framework for a hybrid cloud implementation.



The API management exercise should begin with mapping the database access needs of various application components with the linked business processes, and application workflows besides the user access levels.

In a hybrid cloud environment, requests continuously flow back and forth between public cloud and the data center or private cloud. Therefore, in addition to the standard functions of visibility, availability, and monitoring, your APIs, while acting as gatekeepers, also need to support features such as throttling. When designed with adequate provisioning for caching and fair-use as the guiding principle, throttling can help private cloud administrators achieve performance optimization while measuring resource requests on the business criticality parameters. Allowing developers to request access to a predefined data-set through a developer-portal can also build efficiency into support operations.

Know your organization's hybrid cloud priorities

Hybrid cloud has various usage-driven models. Some organisations build strong data center capabilities and a private cloud relying on public cloud resources only for analytics especially when big data is involved. In fact, this method is similar to the model traditionally followed in third party business intelligence system deployments wherein data fetched from multiple enterprise source systems and ETL is fed into a data warehouse and then to a BI system. In this method, replace BI system with public cloud. The public cloud's access is thus limited to the EDW layer only. The enterprise systems are kept oblivious and out of reach for the public cloud.

Another practice followed by organizations is limiting the scope of public cloud to spike-based provisioning while majority of provisioning being done by the private cloud. Popularly termed as cloud-bursting, the public cloud's role is of augmentative nature only. Through this method, CIOs try to keep their risks and costs under control while ensuring uninterrupted performance at all times.

Lastly, some organizations take a different view of public cloud adoption. By breaking down their applications into back-end and front-end components, the web-based front-end portions are moved to the public cloud while retaining the transaction data processing and analysis at the private cloud level only. An API developer should therefore thoroughly review the practices and risk-return priorities of the organization before creating a suitable API architecture.■

The author is CEO & Co-founder, Postman

Maximizing Gains By Combining New Digital Investments

A new World Economic Forum (WEF) research finds new technologies, deployed in combination, contribute to significantly higher productivity gains when than when they are deployed individually

The productivity increase due to investments in new digital technologies is significantly more when technologies are deployed in combination, finds a new research by the World Economic Forum (WEF). The finding is part of a broader project—Maximizing Returns on Digital Investments—by WEF's Digital Transformation Initiative (DTI) to understand the relationship between new technology investment and productivity.

The research found four key trends:

- The return on investment in new technologies is positive overall. The productivity increase is three times higher when technologies are deployed in combination.
- The return on digital investments varies by industry, and industry leaders achieve a greater productivity increase from investments in new technology than followers. The leaders in a majority of industries tend to be larger companies by revenue.
- Asset-heavy industries realize more value from robotics; asset-light industries realize greater value from mobile/social media.
- While industry leaders realize higher overall return from robotics and mobile/social investments, followers have gained more from IoT and cognitive technologies.

The WEF research identified three key drivers of digital investments: New efficiencies, enhanced customer experience and new business models.

It concluded that new efficiencies are still the primary driver for large companies to invest in new technologies while investing in new business models is the most difficult and least frequently targeted of the three drivers.

The research also identified five key enablers to maximize the return on digital investments emerged from the discussions with industry leaders. They are:

Agile and digital-savvy leadership: Maintaining a strategic vision, purpose, skills, intent and alignment across management levels to ensure a nimble decision-making process on innovation

Forward-looking skills agenda: Infusing a digital mindset in the workforce by making innovation the focus of training and hiring programs

Ecosystem thinking: Collaborating within the value chain (e.g. with suppliers, distributors, customers) and outside (e.g. start-ups, academia)

Data access and management: Driving competitiveness through strong data infrastructure and warehouse capability combined with the right analytics and communication tools

Technology infrastructure readiness: Building the required technology infrastructure to ensure strong capabilities on cloud, cybersecurity and interoperability

As per WEF research, there are three key drivers of digital investments: New efficiencies, enhanced customer experience and new business models.

The project was launched to address the understanding gap that exists in new technologies' impact on productivity.

Some of the questions that it addressed are:

- How much value are companies getting from digital investments?
- How do returns on digital investments vary by company, industry and technology?
- How can companies maximize return from their digital investments?
- How can companies successfully execute on digital investment projects?

The research considered four new technology areas: Cognitive technologies including AI and Big Data; IoT/connected devices; Robotics encompassing design, construction, implementation and operation of robots; and Mobile/social media.

The research combined quantitative and qualitative analysis of new technology investments, data from over 16,000 public companies across 14 industries to estimate the productivity impact of investments in new technologies. The industries were automotive, aviation and travel, chemistry and advanced materials, consumer, electricity, financial services, healthcare, logistics, media, mining and metals, oil and gas, professional services, retail and telecommunications.■

Cryptomining Malware - Impacting Majority of Organizations

According to Fortinet report, cybercriminals are evolving their attack methods to increase their success rates and to accelerate infections

Cybercriminals are evolving their attack methods to increase their success rates and to accelerate infections, according to Fortinet's *Global Threat Landscape Report*. While ransomware continues to impact organizations in destructive ways, there are indications that some cybercriminals now prefer hijacking systems and using them for cryptomining rather than holding them for ransom. Some of the key highlights of the report are:

Cybercrime Attack Methods Evolve to Ensure Success at Speed and Scale

Data indicates that cybercriminals are getting better and more sophisticated in their use of malware and leveraging newly announced zero-day vulnerabilities to attack at speed

and scale. While the number of exploit detections per firm dropped by 13% in Q1 of 2018, the number of unique exploit detections grew by over 11%, and 73% of companies experienced a severe exploit.

- **Spike in Cryptojacking:** Malware is evolving and becoming more difficult to prevent and detect. The prevalence of cryptomining malware more than doubled from quarter to quarter, growing from 13% to 28%. Additionally, cryptojacking was quite prevalent in the Middle East, Latin America, and Africa. Cryptomining malware is also showing incredible diversity for such a relatively new threat. Cybercriminals are creating stealthier file less malware to inject infected code into browsers with less detection. Miners are also targeting multiple operating systems as well as different cryptocurrencies, including Bitcoin, Dash, and Monero. They are also fine-tuning and adopting delivery and propagation techniques from other threats based on what was successful or unsuccessful to improve future success rates.

- **Targeted Attacks for Maximum Impact:** The impact of destructive malware remains high, particularly as criminals combine it with designer attacks. For these types of more targeted attacks, criminals conduct significant reconnaissance on an organization before launching an attack, which helps them to increase success rates. Afterwards, once they penetrate the network, attackers spread laterally across the network before triggering the most destructive part of their planned attack. The Olympic Destroyer malware and the more recent SamSam ransomware are examples of where cybercriminals combined a designer attack with a destructive payload for maximum impact.

- **Ransomware Continues to Disrupt:** The growth in both the volume and sophistication of ransomware continues to be a significant security challenge for organizations. Ransomware continues to evolve, leveraging new delivery channels such as social engineering, and new techniques such as multi-stage attacks to evade detection and infect systems. GandCrab ransomware emerged in January with the distinction of being the first ransomware to require Dash cryptocurrency as a payment. BlackRuby and SamSam were two other ransomware variants that emerged as major threats during the first quarter of 2018.

- **Multiple Attack Vectors:** Although the side channel attacks dubbed Meltdown and Spectre dominated the news headlines during the quarter, some of the top attacks targeted mobile devices or known exploits on router, web or Internet technologies. 21% of organizations reported mobile malware, up 7%, demonstrating that IoT devices continue to be targeted. Cybercriminals also continue to recognize the value of exploiting known vulnerabilities that haven't been patched along with recently discovered zero-days for increased opportunity. Microsoft continued to be the number one target for exploits, and routers took the number two spot in total attack volume. Content Management Systems (CMS) and web-oriented technologies were also heavily targeted.

- **Cyber Hygiene - More Than Just Patching:** Measuring how long botnet infections persist based on the number of consecutive days in which continued communications are detected reveals that hygiene involves more than just patching. It is also about cleanup. Data showed that 58.5% of botnet infections are detected and cleaned up the same day. However, 17.6% of botnets persist for two days in a row and 7.3% last three days. About 5% persist for more than a week. As an example, the Andromeda botnet was taken down in Q4 2017 but data from Q1 found it continued to show up prominently in both volume and prevalence.

- **Attacks Against Operational Technology (OT):** While OT attacks are a smaller percentage of the overall attack landscape, the trends are concerning. This sector is increasingly becoming connected to the Internet, with serious potential ramifications for security. Currently, the vast majority of exploit activity is directed against the two most common industrial communication protocols, primarily because they are so widely deployed. Data shows that in Asia ICS exploit attempts appear to be somewhat more prevalent when compared to ICS exploit activity across other regions.

> Cybercriminals continue to recognize the value of exploiting known vulnerabilities that haven't been patched along with recently discovered zero-days for increased opportunity.

Fighting Evolving Cybercrime Requires Integrated Security

The threat data in this quarter's report reinforces many of the prediction trends unveiled by the Fortinet FortiGuard Labs global research team for 2018 demonstrating that the best defense against intelligent and automated threats is an integrated, broad, and automated security fabric. A highly aware and proactive security defense system is needed to keep pace with the next generation of automated and AI-based attacks.■

A Strong Cybersecurity Infra in 2018 - That's The Focus For Indian Organizations

The aim is to protect data of consumers, suppliers and employees in the wake of increasing data breaches

With data breaches becoming more common than ever, Indian companies are gearing up to strengthen their cybersecurity infrastructure in 2018 in order to protect data of consumers, suppliers and employees, the results of a new survey of chief financial officers (CFOs) shows.

Indian finance executives are likely to increase spending on travel and entertainment and invest on mobile technology, hardware and infrastructure in 2018, showed the "Global Business and Spending Outlook Survey" commissioned by American Express.

Conducted by Institutional Investor Thought Leadership Studio, the survey, which is in its 11th edition, said that 97% of survey respondents from India anticipate an uptick in their companies' headcount in the year.

"India is leading the way in terms of both business confidence and investments," said Saru Kaushal, Vice President and General Manager, Global Commercial Services, American Express Banking Corp., India.

"Businesses are reiterating the need for increasing spend on travel and entertainment, optimising cash flow and using it judiciously to grow and protect the business," she added.

The findings are based on a survey of 870 senior finance executives from companies around the world with annual revenues of USD 500 million or more.

While one third of the Indian CFOs surveyed are likely to spend more on transportation/logistics and 53% on hardware and infrastructure, half of the senior financial executives aim to increase spending on mobile technology, the results showed.

About 40% of the CFOs surveyed said that they are likely to invest more than last year in improving administrative process efficiency to help meet business objectives.

About 87% of the respondents believe that commercial innovations of the so-called "sharing economy" - those used by ride-sharing services like Uber or lodging services such as AirBnB - will have a substantial impact on their industry in the next five years.

About 60% of the executives agreed that their company's travel policy allows employees to use sharing economy services for lodging or transportation when travelling on business.■

Now A New Online Education Program To Empower Female Entrepreneurs

The program, 10,000 women, provides female entrepreneurs across the world with a digitized curriculum and interactive platform of women business owners

The Goldman Sachs Foundation launched an online education program, 10,000 Women, providing female entrepreneurs across the world with a digitized curriculum and interactive platform of women business owners. In partnership with Coursera, the world's largest online platform for higher education, 10,000 Women will provide greater access to its proven curriculum, providing female entrepreneurs with a world-class business education and a global peer-to-peer network. The course is free, and has been built to meet the needs of women business owners in developing markets.

10,000 Women will provide focused and tailored exercises in an introductory module where participants will assess the strengths and weaknesses of their business and themselves as business leaders. The additional modules will review strategies to identify, optimize, and execute growth opportunities. Learners at the end of the course will have a Business Growth Plan to follow as they continue to grow and evolve their businesses.

Importantly, participants in the course will be supported by a network of fellow students and alumni that will provide real-time support, mentoring and group learning across a number of technologies and channels. This is specifically designed to support quality outcomes by driving personal growth and fostering an online community, allowing the participants to create meaningful connections that will last beyond the completion of the program itself.

"This is a question of opportunity, not capability, and this partnership with Coursera allows us to expand 10,000 Women to reach those entrepreneurs we haven't been able to before," said John F.W. Rogers, Chairman of the Goldman Sachs Foundation. "Helping businesses grow is at the core of what we do as a company, and increasing access to business education to support smart, driven, and talented women is good for their businesses, their communities, and the world."

"Supporting women entrepreneurs is so crucial to creating an economic future that is fair and inclusive, and we're so honored to partner with the Goldman Sachs Foundation in this endeavor," said Leah Belsky, VP Enterprise Development at Coursera. "Exponentially scaling this program with our platform will allow many more women to develop the skills, credibility, and networks needed to execute on their ideas."

In 2008, Goldman Sachs launched the 10,000 Women initiative to foster economic growth by providing women entrepreneurs around the world with business education and access to capital. The initiative was founded on research conducted by Goldman Sachs, the World Bank and others, which suggests that such an investment can have a significant impact on GDP growth. 10,000 Women has reached more than 10,000 women though the in-person program, where 70% of graduates report higher revenues and nearly 60% create new jobs.

The course has been built on the foundation of the proven 10,000 Women curriculum with the aim of democratizing access to business education worldwide.

This course has been built on the foundation of the proven 10,000 Women curriculum with the aim of democratizing access to business education worldwide. The announcement follows a recent milestone achieved through a partnership with the International Finance Corporation, a member of the World Bank Group, to enable women entrepreneurs to access capital, with the Women Entrepreneurs Opportunity Facility ("WEOF") raising over USD 1 billion in capital commitments to banks for women entrepreneurs.

The course is free and open to all learners. Women business owners with at least three employees and USD 50,000 in annual revenue are eligible to receive a certificate upon completion. The course can be found at https://www.coursera.org/launch/10000women.■

India Public Cloud Revenue To Rise In 2018

As per Gartner, the growth will be 37.5% in 2018 to total USD 2.5 billion, up from UD 1.8 billion in 2017

The India public cloud services revenue will grow 37.5% in 2018 to total USD 2.5 billion, up from UD 1.8 billion in 2017, according to Gartner.

"While the public cloud revenue market in India exhibits solid growth in 2018, the growth rate is expected to flatten, which is indicative of a maturing market," said Sid Nag, research director at Gartner.

As per Gartner, in 2018, the fastest-growing segment of the public cloud market will be infrastructure as a service (IaaS). IaaS in India will total USD 1 billion, an increase of 46% from 2017 (see Table). This growth is being driven by organizations refraining from pursuing datacenter build-outs and consolidation among datacenter vendors.

"While IaaS enables efficiencies and cost benefits, organizations need to be cautious about IaaS providers potentially gaining unchecked influence over customers and the market," said Nag. "In response to multicloud adoption trends, organizations in India are also increasingly demanding a simpler way to move workloads, applications and data, across cloud providers' IaaS offerings without penalties."

In regions such as India, pricing will be a major factor in organizations' decision making and selection of public cloud providers. "This means that some providers will be at risk if they fail to align their pricing," Nag added.

Software as a service (SaaS) remains the largest segment of the public cloud market in India, with revenue to reach USD 932 million in 2018, an increase of 34% year-over-year.

"Organizations continue the move toward applications and workloads to the cloud locally, as opposed to running them on-premises. Today, SaaS users are increasingly demanding more purpose-built offerings engineered to deliver specific business outcomes," said Nag.

Within the platform as a service (PaaS) category, database PaaS (dbPaaS) is set to be the fastest-growing segment over the next four years. The dbPaas segment is on pace to total USD 32 million in 2018, an increase of 50% from 2017. Gartner expects the segment to reach almost USD 113 million by 2022. This presents a great opportunity for hyperscale cloud providers to include dbPaaS in their service offerings to grow their user numbers.

The rapid growth of dbPaaS is indicative of organizations in India moving away from traditional on-premises, license-based database consumption models to cloud-based "as a service" models, which are generally more price-competitive.■

Table: **India Public Cloud Service Revenue Forecast, 2017-2019** (Billions of U.S. Dollars)

Segment	2017	2018	2019
Business Process as a Service (BPassS)	102	129	155
Platform as a Service (PaaS)	143	191	243
Software as a Service (SaaS)	649	932	1,179
Cloud Management and Security Services	157	201	249
Infrastrauture as a Service (IaaS)	157	201	249
Total	**1,789**	**2,461**	**3,190**

Source: *Gartner (May 2018)*

Note: *Total may not add up due to rounding. The forecast also excludes cloud adverting which was removed from Gartner's public cloud service forecast segments in 2017.*


CFO
INDIA
NETWORK
Intelligence . Leadership . Transformation
A PEER-POWERED,
KNOWLEDGE - BASED AND
COMMUNITY-LED INITIATIVE
FOR CFOs

Blockchain Revolution In Digital Advertising

Blockchain technology, with its clear and traceable audit trails, allow implementation of effective anti-fraud measures to prevent all forms of ad fraud ranging, from basic click fraud to sophisticated illegal traffic

With investigations into the Facebook-Cambridge Analytica scandal resulting in lawsuits and GDPR coming into effect, digital advertising's unbridled collection and usage of user data is finally meeting legal resistance. The digital advertising industry, previously opaque and behind-the-scenes, is finally being pulled out into the light, with the general public waking up to the full reach and power of the industry.

But in today's technologically accelerated age, laws may not be enough to protect user privacy. Current legal frameworks evolved over centuries, whereas today's advances in digital technology, following Moore's law, are growing at an exponential rate.

Andrea Matwyshyn, a professor at the University of Pennsylvania's Wharton School, who tracks the intersection of law and technology points out, "Generally, (the law) is at least five years behind technology as it is developing."

Can Blockchain Fill in for the Lack of Legal Frameworks?

By leveraging technological advances, certain areas can be proactively addressed where laws fail to keep up the pace.

Blockchain technology, the underlying mechanism behind Bitcoin, is one such example. Renowned for ability to keep data secure and anonymous, blockchain keeps an immutable, traceable digital ledger on digital "blocks" linked together through digital cryptography. In the case of Bitcoin, these blocks store transaction data, but in practise, it could store any data.

With the rapid development of blockchain's potential applications across a range of industries, blockchain technology has finally made its way into the digital advertising world. A leading example of this integration is the DATx project, initiated by the Cosima Foundation based in Singapore.

DATx is a project that wishes to build a whole new digital advertising

ecosystem that gives data rights back to users. At the IBM Avazu blockchain salon in Beijing, Mona Du, global lead of business development at DATx, explained the vision in the keynote address: "In the digital advertising industry, users are not respected. They have no say over their own data rights. Through blockchain technology, DATx hopes to achieve greater data privacy and security."

How Can Users Move Beyond Being Passive Participants?

Users participating in the DATx ecosystem can opt into giving their data to advertisers and media platforms to receive DATx token incentives. Furthermore, they are able to select different levels of data authorization for different media channels. This data is gathered, stored, and encrypted on the blockchain. No personal identifying information is collected; behavior data comes in the form of feature tags that are linked to a user's UID, which cannot be traced back to an address or name.

If users opt in to provide their data, users not only get paid for their data, but are exposed to higher quality ads and content they actually want to see.

How Can Media Platforms and Advertisers Benefit from Giving Users Rights to User Data?

However, as they say, it takes two to tango. The DATx project doesn't just give users a fairer playing field in the industry, it benefits all the players in the system, establishing an digital advertising ecosystem incentivizing mutualistic interactions between users, advertisers, and media platforms.

While media platforms and advertisers are now feeling the squeeze from new digital privacy laws, they have also always faced their respective pain points in the traditional digital advertising industry.

Since the advent of websites, media platforms have always had to host ads to pay for their servers, content, and maintenance costs in exchange for website traffic. Services like Adblock became mainstream as a result of the poor quality of advertisements. Paywalls have been set up as an alternative monetization model at the cost of low website traffic.

In addition, with centralization of user behavior data, the "walled garden" phenomenon has arisen. Most media platforms have no access to comprehensive user profiles of the visitors they get, as user behavior data isn't shared across different media platforms. The end result is media platforms are unable to deliver quality ads to their visitors, and have no choice but to host low quality ads.

On the DATx platform, when users opt in to provide their data, media platforms have full access to the user's complete user profile, which includes how they browse and interact with content across the entire range of sites they visit. This allows media platforms to host accurate targeted ads, maximizing eCPM for better monetization of their website traffic, which would also increase without low quality ads and paywalls.

"Half the money I spend on advertising is wasted; the trouble is I don't know which half." Most people in the advertising business have heard this quote, attributed to John Wanamaker, a pioneer in marketing. Almost a century after his death, even with the arrival of digital marketing and programmatic advertising, his quote still remains relevant.

For advertisers, the problem is manifold. Much like with media platforms, they are unable to reach their target audience with precision, as they lack access to accurate user profiles. Even with programmatic advertisements, which essentially amount to automation, precision is still lacking and doesn't allow for customization of ads to effectively connect with the audience.

DATx taps into cutting edge big data analysis techniques and AI recommendation systems to help advertisers find their audience and reach them efficiently.

In addition, click fraud, operated through bots, is rampant within the industry, with many advertisers slowly losing trust in the entire industry itself. The World Federation of Advertisers, whose members include McDonald's, Coca Cola, and Visa, has warned that digital ad fraud is 'endemic'. USD 14.5 billion was lost due to mobile ad fraud alone, amounting to over 10% of all revenue spent on mobile ad fraud in 2017.

DATx taps into cutting edge big data analysis techniques and AI recommendation systems to help advertisers find their audience and reach them efficiently. Furthermore, understanding that native advertising is currently the most effective digital advertising technique, DATx leverages its access to comprehensive user profiles to allow advertisers to employ customized native advertising. All of these results in increased ROI on ad placements for advertisers.

Blockchain technology, with its clear and traceable audit trails, allow DATx to implement effective anti-fraud measures to prevent all forms of ad fraud ranging, from basic click fraud to sophisticated illegal traffic. Utilizing intricate algorithms that can easily verify real human interactions with ads, DATx hopes to eliminate ad fraud on its platform to bring back advertiser confidence in digital marketing.

Lastly, settling payments in DATx token allows DATx to be a truly global, cross border project. As cryptocurrency by-passes the inefficiencies and fees of cross border transactions, all parties participating in the DATx ecosystem are guaranteed secure and rapid payments that are easily traceable.■

More And More Indian Organizations Adopting Augmented Analytics Tools

The change from traditional enterprise reporting is set to positively impact the analytics and business intelligence (BI) software market in India in 2018

Indian organizations are increasingly moving from traditional enterprise reporting to augmented analytics tools that accelerate data preparation and data cleansing, according to Gartner.

This change is set to positively impact the analytics and business intelligence (BI) software market in India in 2018. As per Gartner, analytics and BI software market revenue in India will reach USD 304 million in 2018, a 18.1% increase year over year (see Table).

"Indian organizations are shifting from traditional, tactical and tool-centric data and analytics projects to strategic, modern and architecture-centric data and analytics programs," said Ehtisham Zaidi, principal research analyst at Gartner. "The 'fast followers' are even looking to make heavy investments in advanced analytics solutions driven by artificial intelligence and machine learning, to reduce the time to market and accuracy of analytics offerings."

"We are witnessing a rapid shift to the cloud and hybrid data management through focused data management offerings, including integration platform as a service (iPaaS) tools for cloud integration and data preparation tools for self-service integration," said Zaidi. "We are also seeing the emergence of data lakes and data hubs, as a new way to ingest and manage multi-structured data. However, unavailability of talent will continue to be a major inhibitor toward their adoption."

There is avid demand from Indian organizations to integrate and manage unstructured data, and some are also experimenting with data science on real-time streaming data. As a result, data management software market revenue in India is on pace to total USD 950 million in 2018, a 13.2% increase year over year.

Globally, purchasing decisions continue to move from IT leaders to line-of-business executives and business users who want more flexible, agile and personalized options. "This is in stark contrast to the large, enterprise-scale deals that fuelled double-digit growth at a time when IT had larger budgets and wielded much more influence in buying decisions," said Zaidi.

"In India, CIOs, chief data officers (CDOs), and data and analytics leaders must evolve their traditional approaches," said Zaidi. "They need to focus on business outcomes, explore algorithmic business, and build trust with the business and external partners."■

Table: **Analytics and BI Software Revenue Forecast, India, 2017-2019 (Millions of Dollars)**

Segment	2017	2018	2019
Corporate Perfomance Management (CPM) suites	40.5	46.1	52.1
Analytic Applications	24.8	29.6	35.0
Data Science Platforms	30.0	39.0	50.2
Modern BI Platforms	28,498.2	7.4	12,707.3
Traditional BI Platforms	102.5	107.7	111.5
Total	**257.0**	**303.7**	**356.2**

Source: Gartner (May 2018)

Organizations Adopting More Omnichannel In Customer Experience

Integrated omnichannel support simultaneously leverages channels including email, webform, chat, phone, and self-service

As companies increasingly look to provide a better experience for customers, offering support across multiple channels is becoming more popular than ever. But there's a difference between providing support on a few channels and delivering a truly integrated omnichannel solution.

According to key findings from 2018 Zendesk Benchmark Report, integrated omnichannel support simultaneously leverages channels including email, webform, chat, phone, and self-service. It was found that this approach is not only in line with changing customer expectations - it also means

a tangible return on investment in terms of improved efficiency and an all-around better experience for customers.

KT Prasad, Country Sales Director, Zendesk India, said "India is no different and companies have been increasingly adopting omnichannel customer support in recent years. Based on Zendesk Benchmark data, the benefits of an integrated omnichannel approach are clear. It gives companies a single view of the customer, allowing them to improve operations by ensuring they can refer back to a complete record of past interactions. It's a way for companies to meet customers on the channels they're already using in their daily lives, and it means leaning heavily on live channels, which perform better across key metrics."

Key findings

Omnichannel essentially means more efficient support. Among Zendesk Benchmark companies, those using an integrated omnichannel solution outperform those who stick to a limited number of channels or operate channels in silos. Their customers spend less time waiting for responses, resolve their issues faster, and are less likely to require any follow-ups.

Customers using integrated omnichannel solution spend less time waiting for responses, resolve their issues faster, and are less likely to require any follow-ups.

• Omnichannel companies are better positioned to meet customer expectations: Customers have higher expectations, and they want to be able to move seamlessly across channels. Since 2017, a majority of customers with multiple tickets used more than one channel to reach out to customer support.

• Live channels are being adopted fastest: Live channels, such as Facebook, are growing most quickly, outpacing the growth of traditional email and webform. For integrated omnichannel companies, live channels are on track to surpass email and webform in terms of the share of a support team's workload they represent.

• Live channels also outpace others according to key metrics: Live channels aren't just among the fastest-growing - they also perform better across key operational metrics. Tickets handled through phone and chat support see higher CSAT, fewer re-opens, and faster first resolution times.

• B2C companies are going omnichannel at the quickest pace: B2C companies are more likely to take an omnichannel approach, as they represent the largest share of integrated omnichannel companies by target audience. B2C companies also deal with significantly higher ticket volumes, since they typically have a bigger and more diverse customer base than B2B companies or support desks for internal use.

Customer expectations have never been higher, and by taking an omnichannel approach to support, companies are aiming to meet customers where they already are. That means having a support solution that's fully integrated across channels and provides a personalized experience no matter where the customer is or which device they're using.

The study also found that 61% of respondents surveyed said they were less patient with customer service than they were five years prior. Companies can meet these rising expectations by focusing on customer needs and preferences, regardless of which channel they use to contact support. And it means moving beyond simply providing conventional channels like email and webform, to also offering live channels like phone and chat. Customers are already expecting to be able to more easily move across channels.■

5 Steps Security Leaders Can Take To Create Better Customer Experience

The ability of security leaders to abstract out technology and put decisions in terms of business outcomes is critical to their success in a modern risk-based world

While IT, and most businesses, have been focused on operational excellence for the past 20-30 years, Gartner analysts said it's time security leaders put the focus on customer experience.

"Today, the battle ground for the digital industrial revolution is the customer experience," said Leigh McMullen, research vice president at Gartner. "It's not about cost; it's not about efficiency; it's not even about product. It's about experience."

Everyone is a big digital consumer, and in this digital world, users expect customization to all their preferences. For security leaders, this means giving up some control, and it is resulting in the nexus of the cultural clash. This clash is taking place when risk issues are passed from the business department to the security department, with the expectation that the security team will deal with the problem. Gartner analysts said the key to changing this relationship is engagement.

"We as security people want things to be controlled," said McMullen. "We want them stable, but people's expectations are being set by forces outside our control, which means we (security leaders) need to change how we engage if we want to be successful. We have to give up control to gain influence."

Create an Effortless Experience

The experience that customers are looking for is an effortless experience. The analysts pointed out that effort, not satisfaction or net promoter score, is the best predictor of future buying behavior.

"Security should not wreck the customer experience, but it often does," McMullen said. "Customers, and that

is everyone in your enterprise, want the effort they put in to match the value they expect to get. If you deliver the wrong experience, they'll just tune you out."

Gartner has identified five things security and risk leaders can work on now to create a better experience for their executives. They include:

Actually speak to executives about things that matter to them.

Gartner analysts said studies have shown that fear of risk and security is materially impacting innovation.

"Organizations are slowing down because they fear this issue," said Paul Proctor, vice president and distinguished analyst at Gartner. "If you can improve their comfort and understanding of risk and security, you can help your company move faster. That is truly a business value of security."

Proctor said it's important for security leaders to talk to business leaders about what matter to them. Show them how their business outcomes are directly dependent on technology. He said security leaders need to engage with business executives over things those executives think are important.

Help executives with their decisions through operationally focused risk assessments.

To help business executives, Gartner recommends that security leaders start with a business process and conduct interviews with the people who execute that process.

Gartner analysts shared an example of a police department that has created an operationally-focused risk assessment process that takes two weeks, delivers summary recommendations in a business-focused context, and requires a non-IT executive decision maker to act on the results.

"Offering executives decision-making in the context of operational outcomes makes these engagements more than interesting to them. It directly impacts the decisions they make," Proctor said. "You are now helping them do their job."

Helping executives with their decisions through operationally focused risk assessments is one of the steps security leaders can take to create better customer experience.

Create defensibility for your executives.

Executives do not directly control technology risk and security. However, when an organization gets hacked, the public wants executives to face consequences for the security breach.

"We have treated security like a dark art for so long that when an organization gets hacked, people don't understand," McMullen said. "So, the primary question is, 'Who screwed up?' You can't guarantee the organization won't get hacked, so stop selling your executives protection, and start selling something they truly need, defensibility."

Take tech out of your conversations.

The ability of security leaders to abstract out technology and put decisions in terms of business outcomes is critical to their success in a modern risk-based world. Gartner analysts said security leaders need to understand their company's business model.

"When we talk about technology risk and security, primarily in technology terms, stakeholders treat us like wizards who cast spells and protect the organization," Proctor said. "Making risk and security more transparent and business-aligned is an absolute requirement to get you out of the wizarding world."

Move from project to product management.

Project management is something security leaders have always done. They prioritize and fund activities. For example, there are start times, execution gates, implementation, acceptance testing, integration, and deployments included in project management. There is a beginning and an end.

In product management, everything is continuous. Typically, it's organized around a business process, and the IT requirements to support that business process. For example, in an insurance company, a product line could be underwriting, and in a risk and security context, underwriting needs access to control, perimeter protection, threat and vulnerability management, handling and treatment of sensitive data continuously. There is no end date.

"Doing these five things will improve executive experience, their perceived value, and result in a better, more appropriately protected organization," Proctor said.■

Why The New Digital Communication Policy Should Matter To IT Leaders?

Despite a narrower positioning by Department of Telecommunications, the new digital communication policy is a statement of intent to improve the digital environment holistically...

On 1 May 2018, the Department of Telecommunications (DoT) released the draft National Digital Communication Policy 2018 for public consultation. The latest national communication policy is the fifth overall communication policy document from the government. For long, communication in the country was governed by the Indian Telegraph Act 1885. It took 109 years to get the first national telecom policy of India, in 1994. Since then, this is the third policy statement, the other two having been released in 1999 and 2012.

The significant ways in which it differs from the other three in recent times (1994, 1999 and 2012 versions) is that while all of them were called National Telecom Policy, the current draft replaces 'telecom' with broader and more contemporary 'communication', while 'digital' has been inserted.

The policy is available on the DoT website and is open for public comments, at the time of writing this.

According to the policy document, the policy aims to accomplish the following Strategic Objectives by 2022:

1. Provisioning of Broadband for All
2. Creating 4 Million additional jobs in the Digital Communications sector
3. Enhancing the contribution of the Digital Communications sector to 8% of India's GDP from ~ 6% in 2017
4. Propelling India to the Top 50 Nations in the ICT Development Index of ITU from 134 in 2017
5. Enhancing India's contribution to Global Value Chains
6. Ensuring Digital Sovereignty

While the first five objectives have traditionally guided policymaking in all sectors, the last two—that deal with India's position in the world—are new additions to this policy statement.

Beyond Telecom

When we asked about the policy to CIOs and some senior IT managers, few had any knowledge about what it contains, other than the fact that such a policy has been announced. The only respondent who seemed to be familiar with the policy was from the telecom industry!

While we are not defending the lack of awareness by the IT managers' community, part of the blame should go to the government. Despite being fairly holistic, it has been positioned as just the latest 'telecom' policy.

By its content, specific goals and possible implications, the policy goes well beyond telecom sector. Yet, both its stated objectives—enable creation of a vibrant competitive telecom market to strengthen India's long-term competitiveness—and the channel through which it was released (the administrative department DoT rather than a NITI Aayog or PMO), tends to indicate that it is a sectoral policy.

Take for example, the specific goal, 'establish a strong, robust and flexible' data protection regime, on which the Government has already acted by establishing a committee headed by Justice B.N Srikrishna.

What is 'telecom' about it?

There are three mission statements mentioned in the policy—Connect India (creating robust infrastructure), Propel India (promoting innovation and tech ecosystem and leverage emerging technologies) and Secure India (ensuring privacy, security and digital sovereignty). Only the first part is a logical sequel to previous telecom policies in its scope. The rest two are completely new additions.

In that sense, it is a digitech policy, rather than a telecom policy.

Not too surprisingly, one of the areas for which the provisions have direct implications, is enterprise IT, including information security.

While almost the entire policy has implications for IT, there are several provisions and objectives that will have direct impact on enterprise IT operations (including information security). We have identified 18 such specific points from the draft policy text. You are advised to go through the entire policy at the DoT's website though by the time the issue reaches you, the time for registering your comments would have elapsed.

Here are the 18 points we strongly suggest you need to go through, and take them as inputs while working out your long-term plans. Most of them have positive implications but nevertheless, if you miss them, in a highly competitive market, you may just incur an opportunity cost!

We have indicated the specific clause in the policy within parentheses () against each of the points. This will help you locate them within policy text easily in case you need to understand the context, know specific actions points etc.

Here we go...

#1 Ensuring Inclusion of uncovered areas and digitally deprived segments of society (1.4)

Possible impact: Expansion of access today means expansion of the market. For many products and services, this will give access to new market segments, some of which at the 'bottom of the pyramid'. That itself may foster further innovation!

This is also the only point from the first section of the policy (Connect India) that finds a place in this listing.

#2 Deployment and adoption of new and emerging technologies (2.2.a)

The policy talks about creating a roadmap for emerging technologies such as 5G, Artificial Intelligence, Robotics, Internet of Things, Cloud Computing and M2M by simplifying licensing and regulatory frameworks whilst ensuring appropriate security frameworks for IoT/ M2M.

It also explicitly mentions another emerging challenge—earmarking adequate licensed and unlicensed spectrum for IoT/M2M service.

Encouraging use of Open APIs for emerging technologies is another progressive stance that the policy envisages.

There are three mission statements mentioned in the policy—Connect India, Propel India and Secure India.

Possible impact: Today, most of the experimentations with new technologies like IoT and M2M do not scale up because businesses are unwilling to take the investment risks, because the regulatory directions in a lot of issues including spectrum availability are still unknown. A proactive policy stance like this will open up investments and accelerate the deployment of new technologies.

#3 Transition to IPv6 for all existing communications systems, equipment, networks and devices (2.2.c)

Possible impact: For network managers, especially those managing large and complex networks, everything changes.

#4 Enabling hi-speed Internet, IoT and M2M by 5G rollout (2.2.d)

Possible impact: As sensor technologies become mainstream, the demand for speed will go up exponentially. And most of that speed has to be on wireless networks. So, 5G is a natural evolution. Just that a proactive stance like a policy statement makes the evolution a bit faster and seamless.

#5 Establishing India as a global hub for cloud computing, content hosting and delivery, and data communication systems and services (2.2.f)

The policy promises regulatory frameworks for promoting international data centres, content delivery networks and independent in exchanges in India, while promising a light-touch regulation.

Possible impact: Lower latency, drop in prices and more choice

#6 Leveraging AI and Big Data to enhance the overall quality of service, spectrum management, network security and reliability (2.2.g)

Possible impact: Though it is targeted at the telecom sector, a large and mature sector like telecom can drive down the price as well as help grow skills.

#7 Recognizing Digital Communications as the core of Smart Cities (2.2.h)

The policy proposes developing, in collaboration with Ministry of Urban Development (MOUD), a Common Service Framework and Standards for Smart Cities. There are similar initiatives globally. The government needs to evaluate whether it makes sense to adapt one of these to India or start working on it from scratch, though.

Possible impact: Accelerated smart city rollout will directly impact the volume sales of many technologies like IoT/M2M, Big Data, leading to more use cases, availability of skills and lower cost of these technologies.

#8 Promoting Start-ups (2.4)

One of the important objectives and 2022 goals is supporting start-ups through various fiscal and non-fiscal benefits such as academic collaboration, promoting start-ups in government procurements, measures for application service providers

Possible impact: A vibrant start-up environment leads to better innovation and flexibility of deploying technologies for enterprises.

#9 Accelerating Industry 4.0 (2.8)

The policy lists, among its objectives, creation of a roadmap for transition to Industry 4.0 by 2020 taking a sectoral approach. It explicitly mentions development of markets for IoT/ M2M connectivity services in sectors including agriculture and smart cities components. It also talks of establishing a multi-stakeholder led collaborative mechanism for this purpose.

Possible impact: Faster deployment of robotics, IoT and

The Policy at a Glance

Vision

To fulfil the information and communication needs of citizens and enterprises by establishment of a ubiquitous, resilient, secure and affordable digital communication infrastructure and services, and in the process, support India's transition to a digitally empowered economy and society

Mission	Description	Objective	2022 Goals	Points in our story pertaining to the mission
Connect India	Creating robust Digital Communications Infrastructure	To promote broadband for all as a tool for socio-economic development, while securing service quality and environmental sustainability	a. Provide universal broadband coverage at 50 Mbps to every citizen b. Provide 1 Gbps connectivity to all Gram Panchayats of India by 2020 and 10 Gbps by 2022 c. Enable 100 Mbps broadband on demand to all key development institutions, including all educational institutions d. Enable fixed line broadband access to 50% of households e. Achieve 'unique mobile subscriber density' of 55 by 2020 and 65 by 2022 f. Enable deployment of public Wi-Fi hotspots, to reach 5 million by 2020 and 10 million by 2022 g. Ensure connectivity to all uncovered areas	#1
Propel India	Enabling next-gen technologies and services through investments, innovation and IPR generation	To harness the power of emerging digital technologies including 5G, AI, IoT, Cloud and Big Data to enable provision of future-ready products and services and to catalyze the fourth industrial revolution (Industry 4.0) by promoting investments, innovation and IPR	a. Attract investments of USD 100 billion in the digital communication sector b. Increase India's contribution to global value chains c. Creation of innovation-led start-ups in digital communication sector d. Creation of globally recognized IPRs in India e. Development of Standard Essential Patents (SEPs) in the field of digital communication technologies f. Train/Re-skill 1 million manpower for building new age skills g. Expand IoT ecosystem to 5 billion connected devices h. Accelerate transition to Industry 4.0	#2 through #9
Secure India	Ensuring sovereignty, safety and security of digital communications	To secure the interests of citizens and safeguard the digital sovereignty of India with a focus on ensuring individual autonomy and choice, data ownership, privacy and security, while recognizing data as a crucial economic resource	a. Establish comprehensive data protection regime for digital communications that safeguards the privacy, autonomy and choice of individuals and facilitates India's effective participation in the global digital economy b. Ensure that net neutrality principles are upheld and aligned with service requirements, bandwidth availability and network capabilities including next-gen access technologies c. Develop and deploy robust digital communication network security frameworks d. Build capacity for security testing and establish appropriate security standards e. Address security issues relating to encryption and security clearances f. Enforce accountability through appropriate institutional mechanisms to assure citizens of safe and secure digital communications infrastructure and services	#10 through #18

other similar technologies leading not just to huge efficiency gains but better decision making through data analytics.

#10 Establish a strong, flexible and robust Data Protection Regime (3.1)

While the Government has already taken measures on this regard, like the appointment of an expert committee under the chairmanship of Justice Srikrishna, which has already issued a draft stance document and has taken feedback from public, it is probably incorporated in the communication policy document to show its importance in the overall policy making.

Possible impact: This has major implications for enterprise IT and compliance teams. Compliance with newer provisions like right to forget may need significant efforts including investment.

#11 Assure Security of Digital Communications (3.3.a)

The policy talks of infrastructure security (physical infrastructure, cyber-physical infrastructure, hardware and network elements), systems security (equipment, devices, distributed systems, virtual servers) as well as application and platform security (web, mobile, device and software security).

Possible impact: One more layer of security at the service provider level is good news for enterprises, especially small and medium businesses.

#12 Participating in global standard setting organisations (3.3.c)

The policy talks about establishing comprehensive security certification regime based on global standards

Possible impact: It was a long-desired requirement. A country of over a billion people should have a say in what direction the standards should go.

#13 Formulating a policy on encryption and data retention (3.3.e)

This is a hotly debated issue globally. While the government has made a mention of it in the policy, its exact stance is not known.

Possible impact: A policy with clear guidelines is always better than a vague and ad-hoc approach. But keep your fingers crossed.

#14 Facilitating lawful interception agencies with state of art lawful intercepts (3.3.f.ii)

Mentioned as a sub-point of a clause, this one is tricky. The challenge is not technology always, though it is also becoming one. It is how robust is the process and what real powers do the service providers enjoy to say no to a request that is not mandated by policy bought sought by the enforcement agencies.

Possible impact: Depends on how the policy making proceeds, it may make things easier or far more difficult.

#15 Establishing a Security Incident Management and Response System for communications (3.3.g)

Since communication industry is the basic foundation of a digital ecosystem, it has to be made thoroughly secure. Instituting a sectoral CERT that works in tandem with CERT-in is a welcome step.

Possible impact: More secure infrastructure; also lessons for other sectors

Since communication industry is the basic foundation of a digital ecosystem, it has to be made thoroughly secure.

#16 Enforcing obligations on service providers to report data breaches (3.3.g.iii)

Part of the requirements is to report data breaches, not just to authorities but also to affected users. The breach of data at a major telco in India reported in media sometimes back was a major cause of concern.

Possible impact: A lot but we have to see how much teeth does the legislation will have

#17 Developing a comprehensive plan for network preparedness

Targeted at improving network resilience and disaster response, this will surely help all those who depend on these networks; i.e., all of us.

Possible impact: More resilient infrastructure is good news for all users, be it business users or common citizens

#18 Developing a Unified Emergency Response Mechanism

In a natural disaster-prone country like India, creating a permanent mechanism for emergency response is a welcome step. While many a times it happens because of alert officials, the approach is always ad-hoc. An institutional framework with clearly defined roles and responsibilities, standard operating procedures and technical guidelines will surely go a long way in making disaster response far more effective.

One welcome approach is to force service providers share infrastructure in emergency situations.

Possible impact: Many of the other disaster management mechanisms can be effective if the basic connectivity is available. ■

Double Scoop

Two times the revelation

Swarnali Ghosh

Senior Manager – Business Applications, Eveready

TECH GURU WHOM I FOLLOW

Bastin Gerald

MY FAVORITE HOLIDAY DESTINATION

Andaman & Nicobar Islands

MY FAVORITE DRESS

Saree

A CELEBRITY WHOM I MET RECENTLY

Shreya Ghoshal

A TECH BOOK I'M READING NOW:

Oracle E-Business Suite Manufacturing & Supply Chain Management by Bastin Gerald, Nigel King, Dan Natchek

MY PEER IN THE IT COMMUNITY

Amit Halder

Senior Consultant, TCS

MY FAVORITE GADGETS

Laptop, smartphone, ipad

MY FAVORITE SINGER

Kishore Kumar

TECH SHOWS WHICH INSPIRED ME THE MOST

IBM Think 2018 in Las Vegas and Oracle Partner Day in Kolkata

WRITERS WHOM I LOOK UPTO

Chetan Bhagat, Jhumpa Lahiri

A SPORT WHICH I LIKE THE MOST

Football

Am I Ready to be a CIO? Find out now!

APPLY FOR NEXT100 AWARDS

NEXT100 2018

NEXT100 is an annual awards program instituted by IT NEXT magazine that aims to identify 100 experienced IT managers who have the skills, talent and spirit to become CIOs. The awards process invites aspirants to self-nominate themselves for consideration and qualification for the award.

All NEXT100 award applicants participate in an extensive series of activities that tests their techno-commercial, management and leadership skills. The final selection and nomination of the NEXT100 award recipients is made by a prestigious committee of technology and business leaders (the NEXT100 jury) who evaluate applicants on career accomplishments, professional expertise, skills and potential to be a CIO.

The NEXT100 program culminates in a gala ceremony, where each winner is felicitated with a trophy and citation

75%

of winners have climbed up the ladder and taken up higher responsibilities

You can apply today by scanning the QR code

Organised by IT NEXT

A Brand of 9.9 GROUP

Apply for the NEXT100 today—it could change your life. Go to: **www.next100.in**

Avail a 75%* cashback from APC by Schneider Electric and buy any of the IT infrastructure products to upgrade and improve your Edge IT infrastructure.

Did you know that by 2019, 43% of data generated by IoT technologies will be processed at the edge of a network?

Your mission is to provide operational efficiency to your customers through your Enterprise, Small and Medium Business or Entrepreneurial Start-up. To ensure reliable performance of your facility's IT infrastructure throughout its lifecycle, turn your server room into the IoT-ready on-premise data centers with APC Local Edge solution. Invest today in APC Local Edge solution package and we will reciprocate by awarding you a 75%* cashback to buy any of the IT infrastructure products that can complete your Edge IT infrastructure.

APC Local Edge solution package: APC Smart-UPS™, NetShelter Rack, PDUs and NetBotz (Environmental Monitoring)

Certainty in a Connected World

To know more contact us on

Toll Free - **1800 103 0011, 1800 419 4272**
or
Login at **www.apcindiastore.com/edgecomputing2018**

Life Is On | APC by Schneider Electric

*Terms & Conditions:

1. Customer shall be eligible for the cashback, pursuant to the purchase of the complete Local Edge solution (mentioned below) from the Nominated Channel Partners of Schneider Electric (IT Division) "Company": 1. NetShelter Rack 42U (1 unit), 2. APC Smart-UPS™ Online (1 unit), 3. APC Intelligent Rack PDU (1 unit), 4. NetBotz Environmental Monitoring with sensors (1 unit).

2. The cashback is up to 75%* of the invoice value (Basic Value Excluding All Taxes and Duties) to complete other IT infrastructure (components like Servers, Storage, Networking and Security & Surveillance, Software).

3. Offer valid till 30th June, 2018 only.

Subject to other conditions, call us at 1800 103 0011 / 1800 419272 to know full offer Terms and Conditions.