Opinion | Pg 16

How To Harness The Cascading Effect Of DX

Special Feature | Pg 22

Top 50 CIO Movements In 2018

ITNEXT

FOR THE NEXT GENERATION OF CIOs

Becoming a CISO...and after

The CISO has diverse responsibilities. As the role evolves with new expectations added everyday, the current CISOs owe it to their future generation to define the role more meaningfully.

January 2019 | ₹100 | Volume 09 | Issue 08 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

CISO: In search of an identity

The CISO position is not just evolving, it is in search of an identity. Is the CISO the custodian of organizational information asset? Is he/she the protector of IT systems and assets; Or the chief of compliance; Or the protector of consumer data?

Shyamanuja Das

A few weeks after the white paper on data protection framework in India was published, I wanted to know what the CISOs thought about it. In an event, I posed this informally to more than 20 CISOs, many of them from B2C businesses. Only three knew that such a paper existed. Only one of the three—from the telecom industry—had actually seen the whitepaper. By the way, GDPR was already a buzzword by then but since many of them had nothing to do with GDPR, it remained just that—a buzzword—for them.

I am sure, in a matter of a few months, the Personal Data Protection Bill (hopefully Act), will be one of the most discussed topics among Indian CISOs. Many organizations may opt for making the CISOs the Data Protection Officers, as mandated by the draft bill. The same people who had not heard of the legislation will handle the most important responsibility associated with the new regulation.

Many of the CISOs are already overburdened. When I say overburdened, I am not pointing to the quantity of work but to the diversity of responsibility. Diverse responsibility requires a lot of mind space.

Cyber threats are on the rise continuously. The World Economic Forum, in its 2019 annual *Global Risk Report* has identified two cyber threats—data theft/fraud and cyberattacks—as two of the five most likely risks for the world in 2019.

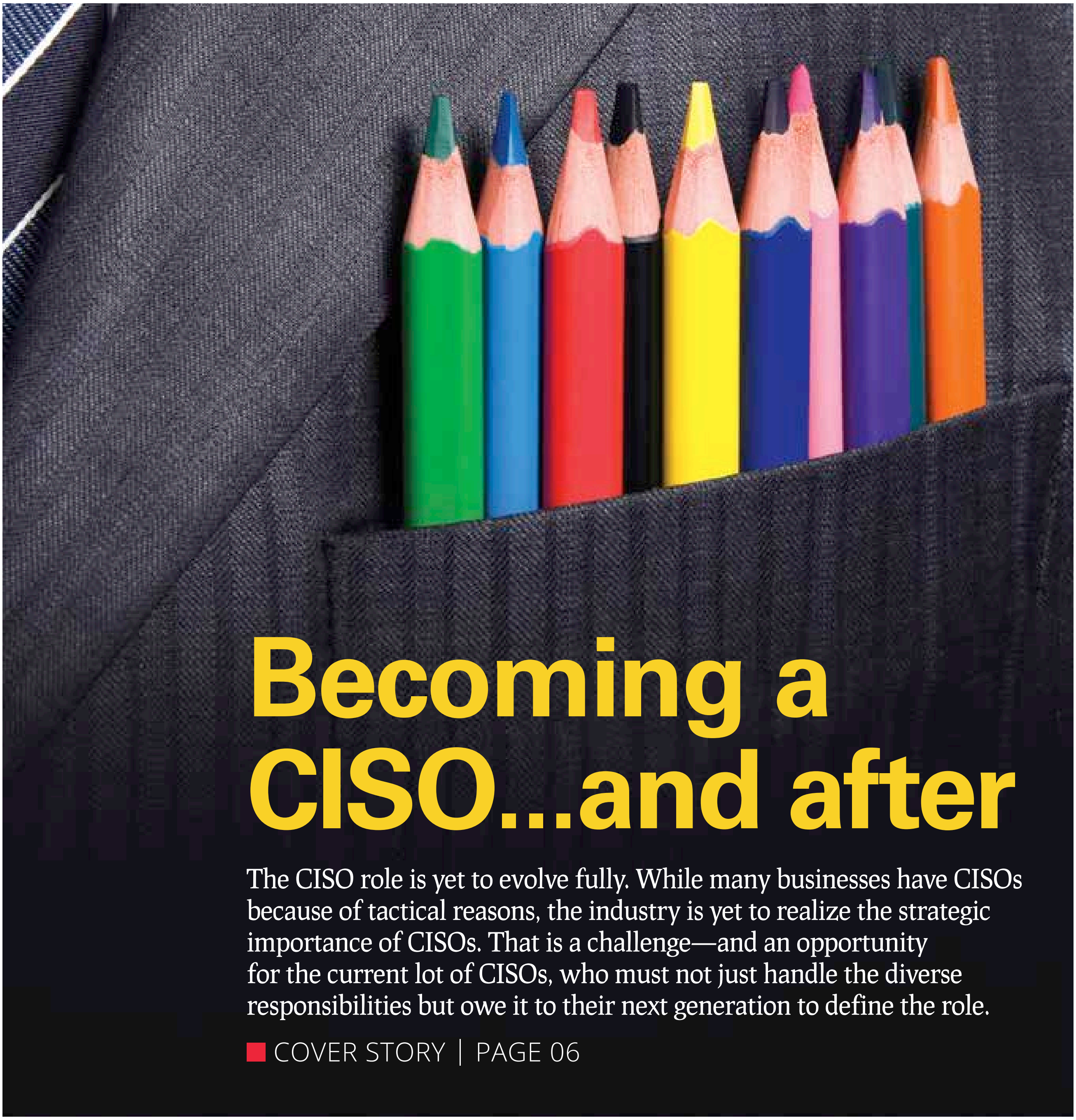
Yet, many organizations are still to realize the strategic importance of CISOs. Many of the regulated businesses—like banking and insurance—have full-fledged CISOs because the regulators in those sectors mandate the positions. They are at a certain seniority level because regulators mandate that. They are outside the enterprise IT department because the regulators specify that. In many businesses where there is no such mandate, CISOs either do not exist as CISOs or report to CIOs. In many cases, CIOs themselves handle the responsibility.

There is a lot of rethinking needed about the CISO position. The position is not just evolving, it is in search of an identity. Is the CISO the custodian of organizational information asset? Is he/she the protector of IT systems and assets; Or the chief of compliance; Or the protector of consumer data?

It is easy to say—all of the above. But these functions have different objectives and have different strategic significance for different organizations. A serious effort of searching for meaningful CISO role is an imperative■

JANUARY 2019
VOLUME 09 | ISSUE 08

Content



Cover Design:
CHARU DWIVEDI

ADVERTISER INDEX

Bry Air Asia	IFC

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

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

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

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

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

Regional Sales Managers
North: Deepak Sharma (+91 98117 91110)
South: BN Raghavendra (+91 98453 81683)
Ad Co-ordination/Scheduling: Kishan Singh

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

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

Editor: Vikas Gupta

9.9 GROUP

An inquisitive mind and a scientific temperament

Wizardry with Wires!

NEXT100 Winner 2017 **PM Dutta**, Senior Manager – IT, Balmer Lawrie, shares his passion for working with electronics as well as his liking for photography and travelling...

Basic electronics have been a passion for me since childhood. The roots of this liking grew big with time. I clearly remember when I was around five years of age, my father gave me the house battery torch to play with as I was down with fever and my family wanted me to take rest for an early recovery. That was the seed of my passion and in no time I managed to collect some wires and learnt the functioning of the switch by shorting the switch with these wires. My dad, a professor of IIT, lovingly answered my queries.

There was no stopping after that. I formed a science club in my school and invited professors from IIT on relevant demonstrations by my friends and seniors. Some of us had our dream fulfilled with a visit to IIT labs.

As I learnt basic circuitry, I was able to understand the circuits of household items like fluorescent tubelights with choke coils and starters, bulbs, geysers, hotplates and iron. My dad encouraged me by increasing my pocket money and a subscription to 'Electronics For You' magazine. I became engrossed in the mechnisms of circuit boards of dancing LED lights, pocket radio, AM transmitters and simple motors and also started mending friends' electronic items.

Then came a sudden turn to my passion. My friend gifted me an old book on audio speakers. The

PM Dutta

Snapshot

PM Dutta is Senior Manager – IT at Balmer Lawrie. He is a NEXT100 Winner of 2017 edition. He has done his PG Diploma in Management Studies and has a certification in Managerial Effectiveness from XLRI-Jamshedpur.

book helped me understand the workings of speakers and its magnets, coil, cone and impedance. I built my first home FIESTA stereo with 10W+10W per channel and initially placed the speakers on earthen water pot to get a significant rise in bass. I tried to transmit the signals but it was jumbled.

My physics teacher taught me the concept of "impedance matching", which initially seemed rather confusing, but encouraged by my teachers I learnt to probe deep. By now, the TV antennae and signal boosters were making sense to me. A nearby TV mechanic taught me the internals of CRT B&W television. The complexity increased with color TV but passion took me through. I started understanding the design differences between German and Japanese circuits, the two technology partners of Indian TV manufacturers at the time.

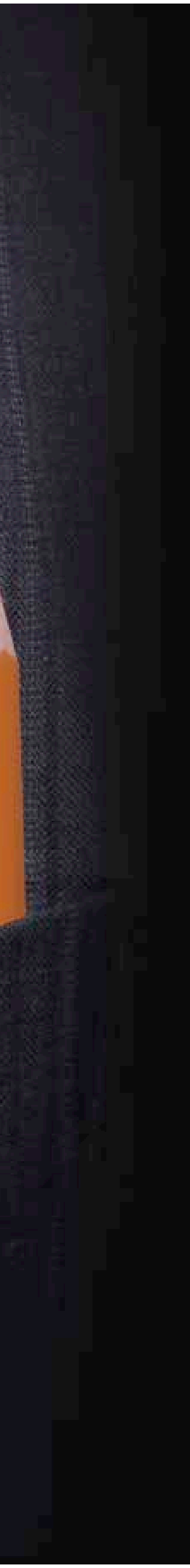
In the meantime the vinyl LP, SP and magnetic cassettes had become a rage in the market. A record company from the UK released vinyl record with 24 tracks, which was recorded at EMI laboratories, UK. I began to wonder, what all this was about? Moreover, what was Dolby Digital? This was the beginning of audio research for me. I developed my first two-way speakers and later upgraded to four-way by changing the audio drivers inside; filling it up with straw as a sound damping factor. I understood about tweeter-midrange-woofer-subwoofers. Then as the technology changed to home theatre from 2.1 to 5.1, 5.2 and 7.1 and more, I learnt the different stages of audio circuitry and pre-amp's. Understanding recording format was also necessary and channelling the tracks to the right kind of speaker was also a requisite. Later on, its quick changes took place in the amplifiers and circuit integration. I was now competent enough to build my own home theatre system.

My experiments with electronics

When I was in my eighth standard, my sister gifted me a vanilla aim-n-shoot 120 format fixed lens box camera. My dad bought books on learning photography, light and shades, aperture setting, film speed and usage of electronic flashlights. My experimentation went on and after I had attained a fair amount of expertise, my dad allowed me to use his 36mm SLR camera with focus. This was a quantum leap for me. As I subscribed to 'National Geographic', I was spellbound by the quality of the pictures and dextrous use of filters in different light and mood situations. I also learnt from various advertisements of world famous camera manufacturers. Getting an imported camera was not easy and so I had to do with a pre-owned camera from a professional photographer. Then came the motorized camera, motorized lenses, embedded software to fine finish the picture and low light photography was further enhanced.

My other hobbies are philately and travelling deep into the Himalayas. My passion has driven me through intricate situations and helped me in my career, driving me to see beyond the horizon■

As told to Dipanjan Mitra, Team ITNEXT



Becoming a CISO... and after

The CISO role is yet to evolve fully. While many businesses have CISOs because of tactical reasons, the industry is yet to realize the strategic importance of CISOs. That is a challenge—and an opportunity for the current lot of CISOs, who must not just handle the diverse responsibilities but owe it to their next generation to define the role. **By Shyamanuja Das**

We, at ITNEXT, have been running the NEXT100 program for 10 years now. Every year, a batch of 100 winners—dubbed as future CIOs—are identified. Many of them have already become CIOs. This is the only program of its kind, which goes beyond the existing set of CIOs to identify the next generation who have the potential to be CIOs. From executives who are below one level of the CIO to who are below five levels, apply for the awards. While requirements of doing certain kind of tasks and handling certain kind of challenges means that people with too little experience rarely make it to the top grade, the winners' list every year typically has few bright guys with just 8-10 years of experience. Caliber and talent apart, these are the guys who are aspiring to be CIOs at that age. "Not surprisingly, we get very large number of applications for the NEXT100 awards—of course, with varying degree of experience and competence" .

Encouraged by the enthusiasm, we started the NEXTCSO awards. While the CISO community—struggling for talent—welcomed it whole-heartedly and participated as jury members enthusiastically, the response from the applicants was no where as enthusiastic. The number of applications is still a healthy 5-6 times that of the winners, but that pales in comparison to the enthusiastic response we get for NEXT100.

Why? Does that mean there is lesser interest for security as a career?

Far from it. Going by certifications and skills upgradations, there is every reason to think that 'security' is the only specialized stream within IT that many professionals can think of.

In the community platforms, security is the only traditional IT area that shares the limelight with the likes of IoT, AI and machine learning.

What explains this paradox? A discussion with a group of young security professionals provided the writer some cues. Admittedly, the idea of the story came from there.

The younger security professionals do not fancy themselves as CISOs. Almost one in every two professionals said that he/she would like to be a security consultant—either independent or join the consulting firms like EY, PwC or KPMG. When specifically asked about CISO, only a handful were excited about the opportunity. In fact, a few of them—the comparatively experienced ones—dreaded the CISO job fearing it would bring to an end their challenging, exciting work and would mean 'running after compliance deadlines.'

In short, far fewer enterprise security professionals dream of becoming CISOs than enterprise IT professionals dream of becoming CIOs. Just 10-12 professionals are too small a sample to draw conclusions from. But it is a pointer to the thinking of these professionals.

The Importance of being a CISO

One of the reasons why CISO is not such a fancied position is not that people do not like the position or job profile, but there is no clear career path to be a CISO. Consequently, there is very little awareness about the position.

In many organizations, there is no designated CISO. There is one Head of Security in the enterprise IT team reporting to the CIO. He/she is a techie familiar with IT security. In some slightly larger organization, the person is actually called a CISO though he/she still reports to the CIO.

It is only with regulated industries like banking and insurance that a designated CISO is mandated by regulation. The regulations further require that a CISO should not report to the CIO because of conflict of interest.

The reason RBI directed that CISOs "should not have a direct reporting relationship with the CIO" is clearly because there is an inherent conflict of interest. The CIO, based on business needs, would like to accelerate the project. The

The Fauji CISOs

Unlike CIOs who almost always grow in enterprise IT or come from IT industry, a lot of CISOs come from others areas—the principal being defense and government. Defense is the single-most source of industry CISOs beyond internal IT.

NAME	DESIGNATION	COMPANY	INDUSTRY	DEFENSE BACKGROUND
A K Anand	Senior Vice President, Global Practice Head & CISO	NIIT Technologies	IT Services	Colonel in Indian Army
AJ Vijaykumar	Ex-CISO	Tata Communications	Telecom	Lt Colonel in Indian Army
Brijesh Datta	EVP and CISO	Reliance Jio Infocom	Telecom	Colonel in Indian Army
Felix Mohan	Erstwhile SVP & Global CISO	Bharti Airtel	Telecom	Indian Navy
Kaushal K Chaudhary	Executive Director - Group Head IT & IS	Lanco Infratech	Infrastructure	Jt Director Systems (Commander of Indian Navy)
Manish Tiwari	SVP & Global CISO	Bharti Airtel	Telecom	Director – CERT, Indian Navy
Mukesh Saini	Head - IT Security	Essel Group	Diversified	Commander at Indian Navy
Murli Menon	CISO	Atos India	IT Services	Commander at Indian Navy
Parthajit Panda	Erstwhile Head - Information Security & Governance	GMR Group	Infrastructure	Commander at Indian Navy
Prashant Veer Singh	Erstwhile SVP, CISO and CIO	Bharti Infratel	Telecom	Officer Commanding Communications (Major) at Indian Army
Vikas Singh Yadav	CISO	Max Life Insurance	Insurance	Corps of Signals, Indian Army

CISO's job would be to ensure that proper security, checks and balances are in place.

Interestingly, this logic does apply to almost all businesses. In any business, the business guys—helped by internal IT—would like to quickly roll out a service or provide extra features to the customers; the CISO's job is to ensure that it is done securely even if it takes a few extra days or one of the features is not available. It is a continuous trade-off leading to conflict situations between the business/IT team and the security team.

Yet, in most businesses, the Head of Security does report to the CIO. It is not that organizations do not know that the inherent conflict exists. It is a classic case of convenience winning in the convenience-rightness trade-off.

Going forward—does the balance change? That is a question each organization must answer for itself. Interestingly, the various structures that exist for organizational information/cybersecurity are directly derived from examination of this question. Needless to point, some of them are transitionary structures.

Top CISO Movements in India in 2018

Like CIOs, quite a few Chief Information Security Officers (CISO) too moved to newer opportunities in 2018. If the list looks smaller, it is because the overall list is smaller—there are far lesser people with a CISO designation.

Here is the list, presented alphabetically by CISO names with information on the new assignment, immediate past assignment and month of change:

- Abhilash Balan took over as CISO at Bharti AXA General Insurance in December 2018. He was earlier with Kotak Mahindra Bank.
- Akhil Verma took over as CISO of Airtel Payment Bank in November 2018. He was the Senior General Manager and CISO in Fincare Small Finance Bank before this.
- Akhil Wadhavkar joined as CISO in Suryoday Small Finance Bank in May 2018. He was with BSE.
- Anuprita Daga has joined as President and Head of Information Security Group at Yes Bank in October. She was earlier CISO of Reliance Capital for more than five years
- Bhavesh Kumar Pandey joined as CISO of Hero FinCorp in April. He was earlier with MedusInd.
- Deepak Mande joined as CISO of ICICI Lombard in July. He came from ICICI Bank.
- Dilip Panjwani joined as CISO and IT Controller at Larsen & Toubro Infotech in February. He was Director - Information Security at FIS before this assignment.
- Fal Ghanacha joined as the CISO in Aegon Life Insurance in June. He was earlier with Reliance Nippon Life Asset Management.
- Hiren Pandya took over as CISO at Liberty General Insurance in August. He was with Reliance Industries before that.
- Kalpesh Doshi joined as the CISO, India at FIS in August. He was CISO – APAC with Capgemini immediately prior to this assignment.
- Maya R Nair joined as CISO at Reliance Capital in October. She moved from Idea Cellular where she headed information security.
- Oscar Pereira took over as the CISO of Cigna TTK Health Insurance Company. He was earlier handling IT infrastructure in the same company.
- Prasad G joined as CISO of DHFL General Insurance in August. He served for more than seven years at HDFC ERGO Gneral Insurance, including a one and half year stint as CISO.
- Santosh Gupta assumed the responsibility of CISO at Future Generali India Insurance Company in September. He came from Ocwen Financial Corporation.
- Satyanandan Atyam joined took over as Chief Risk Officer at MAX BUPA Health Insurance in August. He was earlier Head of Risk Management, Data Protection Officer and CISO at Bharti AXA General Insurance

The Many CISOs...

The raisons d'être of a CISO post often decides the responsibility handled and power enjoyed by the occupant.

Broadly, the CISOs can be divided into two classes: Industries where the position is needed for a business acquisition/regulatory reason and industries where there is no explicit requirement/mandate for a CISO.

Regulation/Customer acquisition demands it

1. Mandated by regulation: There are some businesses where a CISO post is mandated by the regulation. Often, the minimum level of CISO is defined too by regulation. These businesses have no option but to appoint a CISO. The major examples of these industries are banking and insurance. In both, it is also mandated that the CISO should not have a direct reporting relationship with the CIO. Naturally, each of the banks and insurance companies have a full-fledged CISO and they report to organizational risk function.

2. Not mandated by regulation but stringent compliance requirements: There are other industries where a CISO position is not mandated by regulations, but the industries are fairly regulated, and compliance is a big task. These businesses too have usually full-fledged CISOs with certain power. The examples include telecom, non-banking financial services, and pharma. In Reliance Jio, the CISO reports to the board.

3. Competitive requirements: In some businesses, there may not be any regulatory requirements, but basic business models demand that you should have a CISO. The most prominent example of this type of business is IT/ITES industry. Any company worth its name in this industry would have a senior level person serving as CISOs. During due diligence and even vendor evaluation, many of the clients insist on talking to the CISO, among others to ensure that the processes or IT work that they outsource, are fully secure. Interestingly, with GDPR coming in many markets, the need for personal data protection is becoming important, especially for BPO companies dealing with European citizen's personal data. Often, the GDPR rollout and the responsibility of personal data protection is the CISO's responsibility.

No mandate/No need of parading

Most of the other industries do not have to appoint a CISO for satisfying a regulator or a client but increasingly a CISO position is becoming imperative. One of the top reasons is compliance—not just with regulations but also with numerous organizational governance requirements.

However, in these industries too, various structures exist:

Should CISOs be the Data Protection Officers?

By Sanjivan Shirke

India's privacy legislation is in the making. The draft Personal Data Protection bill has already been released for public comments.

Section 36 of the draft bill mandates that each data fiduciary—entities dealing with personal data of individuals—should have a Data Protection Officer (DPO). Clause 2 of the same section also makes it clear that the position of DPO does not have to be exclusive. An executive with other responsibilities can also carry out the responsibilities of the DPO.

Since the fundamental responsibility of the position is to ensure that individual data being handled by the organization is well-protected, the role will be all about information security and of course, ensuring compliance. As of today, both these roles are handled by the CISOs. The data protection bill just expands the scope to include the data of individuals handled by the organization.

From an organization's point of view, there are broadly two options—either to appoint a legal professional or to appoint an information security professional. In many American and European business, there are the privacy officers who do similar roles. Many of them are legal

professionals. However, in India, legal professionals with the kind of technology understanding the role demands are rare to find. My guess is, most organizations will turn to information security professionals for the job.

From CISO's point of view, is it a good idea to take up the role? It depends on what kind of jobs you love. The DPO role will have three broad responsibilities:

- To ensure that the laws are adhered to using tools and technologies. This is similar to traditional CISO role.
- To be the point of contact for the regulators. It is not the traditional role of CISO but increasingly, they are getting exposed to this.
- To be the point of contact of data principals (consumers). It is a completely new kind of responsibility for the CISO.

However, there is another requirement. Those CISOs who are part of the CIO organization will have a tough job balancing between conflicting responsibilities! Only those CISOs who report directly to CEO/COO/CFO or Head of Risk can effectively carry out the responsibility!

If you think you will love these challenges, go for it. But one thing is for sure, whether you are the DPO or not, you will have to play a big role as the CISO to ensure that your organization is compliant with the provisions for the privacy laws.

The author is Senior Vice President (Information Technology), UTI Mutual Fund. Inputs for this article has also come from Vaibhav Gupta, Technology Solutions Leader- Cyber Security, Microsoft and Terence Gomes, Enterprise Cybersecurity Executive, Microsoft

A. Independent CISO/Reporting to risk: Some businesses do recognize the role of an independent CISO and have appointed independent CISOs. Outside the industries mentioned above, this kind of positions is still relatively rarer.

B. CISO reports to CIO: In some organizations, there is a designated CISO, who reports to the CIO. We believe most of these are interim arrangements. These are in a transition phase from model C.

C. No CISO, an Information Security Head, reports to CIO: This is the model that exists in most of the Indian companies that do not belong to the above-mentioned industries or have not yet identified security as a strategic priority.

D. CIO/CISO roles converge: This is the structure in companies where there is a great need for IT security but comparatively lesser need for data protection/thwarting targeted attacks, etc. The difference between this model and model B could be because of a few reasons, such as decision-making power at a certain level, sheer unavailability of the right people or the CIO coming from a strong security background and not letting it go.

Of course, we are ignoring companies where there are no CISOs. Such companies are becoming rarer by the day. We believe increasingly, models B and D will give way to A and C. A model A CISO would be similar to the CISOs in the industries where a CISO position is a tactical requirement (such as compliance or marketing) too.

Today, the issues that the first category of CISOs and the first sub-category (model A) CISOs from the second category discuss and what the rest discuss are very different. They are also part of the most action. Look at the list of top CISO movements presented in the box. All the 15 movements involved the first category and 13 of the new appointments in the list are in banks or insurance companies, where a CISO position is regulation-mandated.

In short, CISOs are still a new breed in other businesses.

One development—ironically regulatory—may change that. With the personal data protection (individual privacy) bill in India, in the lines of GDPR, on the anvil, it is just a matter of time before most businesses, especially the B2C companies, will come under these regulations and they will have to designate a Data Protection Officer (DPO). With the draft regulations making it explicitly clear that the DPO role need not be exclusive, many would like to have an executive who is good at technology and compliance, handling the job. Many companies who were unable to justify the investment in a full-fledged CISO can easily justify a CISO who also happens to be the DPO, or should we say it the other way round?

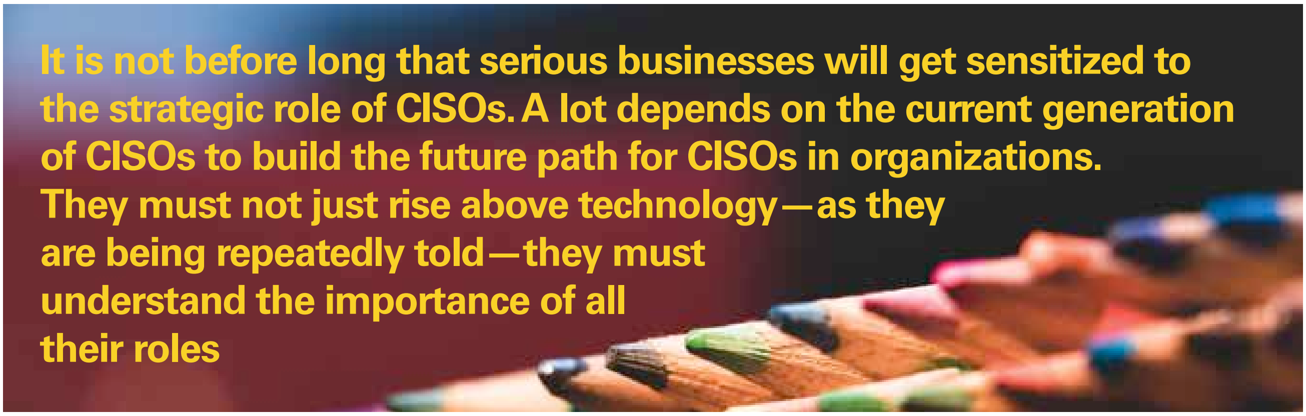
...and their many roles

There is so much discussion around how a CIO needs to be a multi-tasker—handling multiple strategic and tactical things at any point of time. While that is true, the responsibility of CIO, however, is one and can be precisely defined. And that is: Leveraging technology to create value for business.

A CISO, on the other hand, has to perform tasks that have different objectives.

The first—and the stated—objective is to protect organizational information asset. That is supposed to be his reason for existence.

The second—which has become a significant part of a CISO's responsibility—is compliance. While it started with security compliance (an extension of the role), this has now expanded to include all kinds of compliance. However, with organizational and business maturity, this role may move to specialist compliance executives, who would still be part of the broader risk, compliance, security and governance organization, along with the CISO. However, for the time being, it is the CISO who is playing the role.



It is not before long that serious businesses will get sensitized to the strategic role of CISOs. A lot depends on the current generation of CISOs to build the future path for CISOs in organizations. They must not just rise above technology—as they are being repeatedly told—they must understand the importance of all their roles

Third emerging role is going to be protecting the personal data of consumers, once the personal data protection regime sets in. Initially, it will be doing stated work—more like compliance work—but then will evolve to be a full-fledged work. We will see if this too evolves to a separate role. However, initially it is expected that CISOs will have to play the role of data protection officers.

Of course, while these are clearly different roles, the stated role of protecting organizational information has also changed over the years adding far more complexity.

Two of the most fundamental changes have been:

a. Change from an effort-based responsibility to an outcome-based responsibility: With targeted and sophisticated attacks, a CISO's job is not just to build high walls and expect that everything will be fine but to get into the combat mode, matching wits with the attackers. That is a very different ball game.

b. Change from protecting IT systems and information to ensure the business runs: A CISO's job has traditionally been to protect information/intellectual property and IT infrastructure. With digitalization, almost all aspects of a business—manufacturing to retail—is getting automated using information technology. Protecting that is also expected from CISO. Interestingly, in many manufacturing companies, the operational teams do not expect the involvement of CIO in their technology management even if it is significantly digitalized, but they still expect CISO's help to protect that digitalized infrastructure.

The Challenge or the Opportunity?

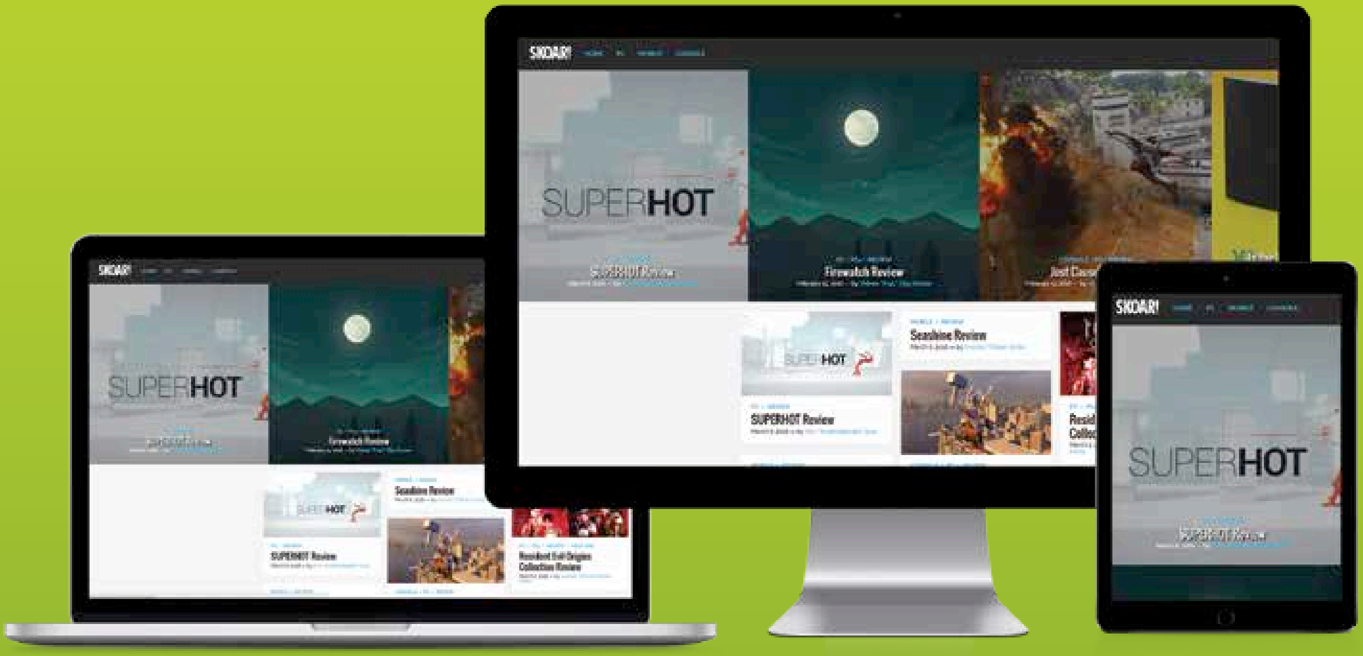
The World Economic Forum (WEF), in its recently released *Global Risk Report 2019,* has identified massive incidents of data fraud/theft and large-scale cyberattacks as the 4th and 5th probable global risks among its top ten most probable risks. It has also identified large-scale cyberattacks as the 7th most impactful risk.

It is a no-brainer that organizations need far more preparations in terms of security to sail through in an era like this. Yet, most organizations do not comprehend the reality so well. Even in industries where CISOs are given power and responsibility, it is driven by tactical considerations like regulation and showcasing to customers.

It is not before long that serious businesses will get sensitized to the strategic role of CISOs. A lot depends on the current generation of CISOs to build the future path for CISOs in organizations.

They must not just rise above technology—as they are being repeatedly told—they must understand the importance of all their roles—their short and long-term implication and build strategic direction for themselves and the next generation security professionals who want to take up this important role of protecting the organization of the future—in many possible ways.

Thanks to its symbiotic relationship with regulation and consumer mindsets, the CISO roles in each of the market will be very different from each other—far more than the difference in CIO roles. That means, today's generation of CISOs has the added responsibility of being role makers■


SKOAR!
SUPERHOT
SUPERHOT Review
Firewatch Review
Just Cause
Seashine Review
Resident Evil Origins Collection Review

Do Indian Organizations Understand The Need To Sync Technology Adoption To Internal Fraud Controls?

Organizations will have to undertake comprehensive fraud risk assessments to identify specific fraud schemes and risks applicable due to adoption of new technologies

By Nikhil Bedi

Over the past few years, organizations in India have adopted technology in most of their business activities, including their anti-fraud efforts. Our previous fraud survey in 2016 identified artificial intelligence, machine learning, robotics and blockchain as technologies for the future. As opposed to that a quarter of the respondents to the current edition of the *India*

Corporate Fraud Perception Survey 2018 have indicated that they are already in the process of implementing technologies.

While adoption of these technologies can definitely bring benefits to the business, in recent times, a lot of new technology adoption has inadvertently facilitated fraud, because the internal fraud controls framework possibly did not keep up with the change in business process that came as a result of new technology adoption. Innovative fraudsters have been using techniques to analyse communication patterns from phishing attacks to facilitating data leak, IP theft and much beyond.

Future fraud will rely on a combination of devices and methods. To tackle future fraud, organizations need to understand that the probability of being defrauded will increasingly depend on the following aspects:

The organization's extent of technology adoption: Organizations with multiple processes that have been automated may be likely to have an increased risk of fraud depending on the area and context of automation undertaken. For example, the RPA process to check for customer emails and respond with an invoice copy can be misused to facilitate data leakage or IP theft.

The organization's technology exposure: The convergence of IoT devices, machine learning and innovative text mining methods has made it easy for fraudsters to identify areas of vulnerability within organizations. Businesses with internet facing, web-based, data driven models can be misused to manipulate information and mislead users. For example, multiple bots programmed to hedge a stock can possibly create influence in supply and demand, and therefore manipulate the pricing of a stock.

The organization's adoption of nascent technology: Most organizations tend to adopt multiple technologies for different processes, with each such technology being in a different stage of maturity. Often when interconnected, the relative immaturity of one technology when pitted against the maturity of another can result in security gaps, exposing the organisation to fraud. For instance, an image similarity algorithm deployed by an insurance company to detect pre-existing damage, can be fooled by adjusting the brightness of the picture, and can significantly alter the decision-making process.

While adoption of these technologies can definitely bring benefits to the business, in recent times, a lot of new technology adoption has inadvertently facilitated fraud

An effective fraud risk management function will have to take into consideration the above aspects and ensure that relevant changes are made in their own processes and internal controls. Organizations will have to undertake comprehensive fraud risk assessments to identify specific fraud schemes and risks applicable due to adoption of new technologies. Further, regular employee education and advisory on new frauds is necessary to create a climate of vigilance.

Lastly, while technology can offer great opportunity to limit frauds if rightfully adopted and implemented, it cannot prevent fraud by its mere existence■

The author is Partner at Deloitte India

How To Harness The Cascading Effect Of DX

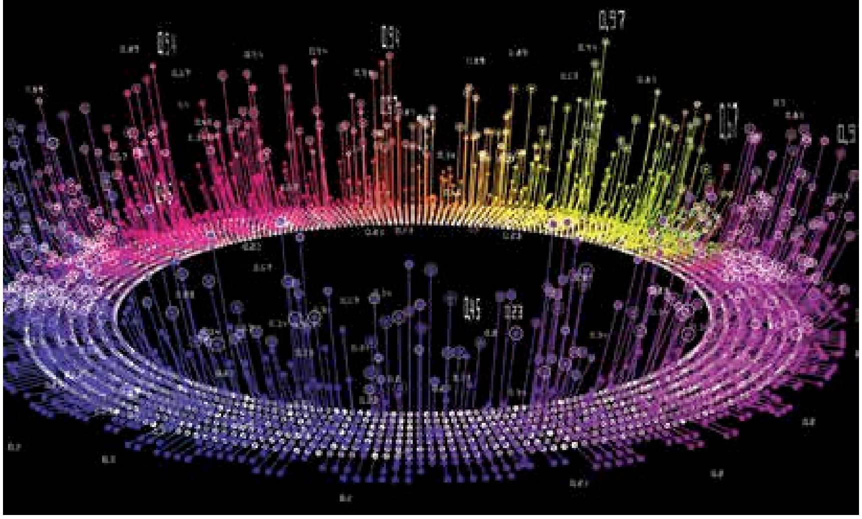
The cascading transformation is an intricate strategic switchover from the legacy systems to cloud-harnessed computing, keeping the line functions seamlessly running without interruption

By PM Dutta

We all understand now that 'change is the only constant'. Digital disruption (transformation) colloquially termed as 'DX'ing is a new dimension to this change. 'DX'ing is focussed to create an edge and value addition to the bouquet of upcoming trends in business models and to bridge customers to etch out a business edge and gain DX competitiveness in the corporate realm.

There has been a significant change in the middle tier of businesses like entertainment, pharmaceuticals and service industries. 'DX'ing has been relatively slower in making an inroad in core manufacturing companies. The ripples of change are being felt and the industry is aligning in anticipation of this change. Government services like metrological department, agricultural research, railways, etc., are churning out petabytes of data and have a tremendous potential to harness the strength of preferential cloud architecture in a mixed mode – the hybrid cloud.

Smart cars, smart homes and every smart device requires seamless uninterrupted data from multiple interfaces to meet the challenges of the day. This high band of data harnessed will bring prudence into decision-making



The Gen-X trend must remain in tandem with real time data to make timely and prudent decisions. Smart cars, smart homes and every smart device requires seamless uninterrupted data from multiple interfaces to meet the challenges of the day. This high band of data harnessed will bring prudence into decision-making and smoothen delivery of services.

The cascading transformation is an intricate strategic switchover from the legacy systems to cloud-harnessed computing, keeping the line functions seamlessly running without any interruption. This stage of transformation calls for close working with the line managers to make the mould of 'DX'ing. In this transition the prima facie role of IT team is to keep the legacy systems intact and manage the change to avoid direct revenue loss due to any form of business continuity disruption.

The next point to focus on is the policy of scalability and the extent of scalability to the cloud on successful porting of the legacy systems, with cost optimization in pay-for-use and the agility for enhanced efficiency. Doubtful reciprocation will have a regressive effect on the cost-benefit analysis in a typical scenario of a hybrid multitier IT architecture. A major hurdle faced here is to synchronize the dual or multiple cloud landscape to a common production perspective. The deployment strategy should harness the change management skills of the steering committee and the development team integrating with the power users, delicate hand-holding, purposeful user training. Rigorous adherence to quality standards is the mantra of success.

Next is the managing of cascading effect on the in-house team and help them to adjust to the newly distributed development platform. There will be switching of APIs, and databases, establishing cross verification of data over multiple clouds which often lead to an intricate situation of managing the development and delivery of the service in schedule. This interfacing however can be reduced by customized on-time coding and search for available codecs to minimize the time, effort and cost.

As we near the close of 'DX'ing technology, the security on cloud has always been a grey area of concern to organizations, exposing vital business data over the hybrid IT architecture and a backward integration with on premise legacy data. This integration itself becomes an intricate challenge. Resolution of these challenges will take us towards the era of digital transformation. An era with new paradigm of advantages that is maturing with time■

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

Why Organizations Must Focus On The Increasing Role Of UX/CX In Their Digital Transformation Journey

As customers strive to expect more, they will handshake only with partners/vendors that embrace this and deliver it through meaningful experiences. For organizations then the question arises as to who should be the right people they sign-up to be part of their journey?

By Nilesh Gupta

Today, startups that build tools for businesses looking to automate their customer service experience and operations are being acquired by global companies. Though they may have the necessary automation tools that may be required during the digital journey, they may not necessarily have the experience to accelerate the digital transformation itself.

User/Customer Experience (CX) is the most important element in the journey of digital transformation that every organization should be striving to improve. Today AI drives almost every aspect of your shopping experience wherever or whoever you are. The dominance of user experience in retail, healthcare or banking verticals are due in part to its mastery of artificial intelligence (including the decision-making process) and to the ability of machines executing your request that was once the purview of humans alone. But then the question arises as to who should be the right people you will need to sign-up to be part of your journey? As customers we strive to expect more, and we will handshake only with partners/vendors that embrace this and deliver it through meaningful experiences.

Nowadays, most enterprises in their journey are not on a single digital platform. They're on disparate platforms with number of different channels. For example, during our visits to different customer offices, we have witnessed enterprises using multiple tools that form their unified communication standards. Now if enterprises have to deep-dive and bring in their own teams to learn and then chalk out the DX roadmap, it could turn out very expensive or the ROI will take forever to be effective. Collaboration of these instant-messaging or other in-house communication channels used with another programmable based API (Voice, Data, ITSM, etc.) is something a managed service provider (MSP) will bring in the experience to integrate with all the components that form the part of the unified communication.

Secondly, the digital infrastructure that will be required as part of the digital transformation is often comprehensive and will require a right service provider to stitch the solutions from many CX based solution partners that will form the full technology stack along with base infrastructure. This includes everything from managing the security and network for various omni-channel to rolling out AI and machine learning solutions to enable true digital transformation. I believe that enterprises will take more proactive steps to engage with the right service provider that has experience in bringing both sides of experience to empower their employees on how technology can change their everyday lives by embracing the DX journey.

Thirdly, with the way technology is behaving by evolving everyday as against a decade ago, managed service providers need to understand the enterprises ever changing business conditions and respond with a holistic solution during and after its DX transformation journey. Besides the one-time implementation strategy, a continuous improvement enhancement to analyze and inventory the CX environments on a regular basis, typically every quarterly will help to evaluate the validity of outcome when compared to its competition in the marketplace.

Enterprises that plan in taking the plunge into digital transformation journey will need to have a strong relationship with IT managed service partner who can successfully guide them in adapting the new way of services model in this digital age■

The author is Vice President & Global Head - Digital Infrastructure Managed Solutions & Strategy (IMS), 3i Infotech

Cyber Security In India – The Year That Was

Breaches, stringent compliance requirements, a false sense of security and lack of skilled manpower mark the challenges for C-level executives in large enterprises

By Shree Parthasarathy

Top concerns: Lack of skilled cyber security professionals; SMEs not prepared to pre-empt and manage cyber-attacks and data breach; Humans remain the most common threat to security of businesses.

India over the past year has seen a sharp increase in the incidence of data breach and cyber-attacks across sectors and company sizes. While the large organizations have been able to contain the damage in most cases by pre-empting attacks on their systems through resilient security systems, in other cases the media has got the whiff of it first. Additionally, the smaller enterprises are the ones who have emerged to suffer the most from irredeemable loss to data and reputation.

Here are some of the key challenges faced by SMEs and C-level executives this year:

Small to mid-market trending business challenges as of 2018

1. Hackers are aware of the complacent nature of small businesses when it comes to cybersecurity. They understand that small businesses invest little-to-no money on improving their

cybersecurity situation. Ultimately, it gives an easy opportunity for attackers to exploit.

2. Larger organizations typically have a robust defence system that is difficult to compromise or breach. However, many larger organizations have systems interconnected with small or mid-size businesses. When hackers compromise the security system of SMEs, they can then easily penetrate into the defence systems of larger organizations.
3. Data breaches can often mean doom for small and medium-size businesses. As a result, they are more vulnerable to ransomware attacks because they are highly likely to pay the ransom to save their data and their company from doom.

Business challenges trending amongst cyber SMEs as of 2018

1. IoT has most definitely added convenience to hectic schedules. However, it has also opened new doors for cyberattacks. It is imperative for employers to now ensure that all IoT devices are set up correctly and there's no room for a network breach.
2. Humans remain the biggest and most common security threat to businesses of all sizes or industries. There are many cases of employees abusing their privilege access, harming the company's security layers in the process and resulting in a huge loss. According to a 2016 survey conducted by Ponemon Institute, 22% of businesses blamed cyberattacks on insiders. Moreover, the same survey also revealed that 56% of businesses reported that the attacks were either by new joiners or employees leaving the company.
3. The flexibility and scalability that the cloud offers makes this technology more compelling to small and mid-size businesses. However, huge concerns still exist for SMEs when it comes to the security challenge associated with the cloud technology. Although cloud technology is getting more and more secure, new and bigger vulnerabilities, loose ends make for security concerns.
4. App consumers are now being tracked through the use of ultrasonic tones. These tones are almost completely silent and can't be picked up by the human ear, but there are apps in your phone that are always listening for them. The technology is called ultrasonic cross-device tracking, and works by emitting high-frequency tones across ads and billboards, web pages, and across retail outlets, etc. Apps with access to the phone's microphone can pick up these tones and build a profile about your viewership details and in some cases even the websites you've visited.

Challenges for C-level executives between 2017 and 2018

1. *Getting compromised and the media catching it first:* Till date, reputation loss due to data breaches proves to be one of the top concerns for C-level execs across all multi-national organisations. Ian McClarty, CIO, PhoenixNAP Global IT Services says that the hope is to "'catch' this breach in a reasonable time to limit and mitigate so that we can notify the victims/public through a controlled message".
2. *GDPR introduction to Europe:* The hottest topic till date amongst most cyber security developments in Europe is the introduction of GDPR.

Humans remain the biggest and most common security threat to businesses of all sizes or industries. There are many cases of employees abusing their privilege access...

A significant change to how personal data is being and will be stored is yet to determine how companies will interpret guidelines on the data they keep based on having a 'legitimate interest' vs. that of requiring explicit 'consent'.

3. *Having a false sense of security:* Given threat profiles for cybersecurity and the need to protect intellectual property and financial assets etc., there is no single investment or method that allows one to 'check the box' and be rid of cyber risks. End-to-end visibility of one's technology footprint—from device to application destination—is a key capability required to enable success in understanding security positions and identifying new attacks.
4. *Lack of cyber security skills amongst employees:* People within a firm, till date, tend to be the highest risk factor across all organizations. With the ever-changing landscape of cyber and information security regulations, C-level execs are finding it increasingly difficult to monitor, advise and implement security guidelines for their employees. Phishing, shared WI-Fi, the GDPR regulations, etc. all are proving to be pain areas for ExCo members as most employees are still not aware of the threats involved■

The author is Partner, National Leader-Cyber Risk Services, Deloitte India

Top 50 CIO Movements In 2018

There was a lot of action in 2018 with many CIOs changing companies and industries. Here is a list of top 50 movements...

CIO stands for Career Is Over—that is how the old quip went. Once you become CIO of a fairly large organization, you are stuck there for long. The joke was not entirely off-the-mark. Many Indian CIOs continued (not always 'stuck') for long in the same organization. The more adventurous of the lot changed jobs—but by and large stuck to same or allied industries. So, you had telecom CIOs or manufacturing CIOs or pharma CIOs. That started changing in 2016 when a significant number of CIOs changed the job they held for more than five-six years, sometimes even longer. It accelerated in 2017.

In 2018, this trend—of CIOs changing their jobs in large numbers to join newer companies, newer industries—got further diffused across Indian industry. A large number of CIOs changed their jobs in 2018.

A few retired too. Some such luminaries who bid adieu to corporate CIO positions include K K Choudhary, an ex-defence personnel, who served as CIO and CISO at Lanco; Praksh Paranjpe of Idea Cellular; Pratap Gharge who retired as the Executive President & CIO of Bajaj Electricals after a long and illustrious innings at the company and Rupinder Goel of Tata Communication, another industry veteran.

We have drawn a list of top 50 CIO movements. These 'movers' are either joining a new company or taking a significantly different and bigger responsibility within the same company. Simple designation changes with marginal tweaks in job descriptions are not part of the list. Since the focus is on CIOs, the list is presented alphabetically on CIO names and not company names or according to date/month which looks pretty mechanical. However, you will find their new designation, new company, immediate past designation, immediate past company and month of change in most cases.

Top 50 Movements

1. Ajay Vij took over as CIO Fortis Healthcare in October 2018. He was earlier handling Supply chain management in the same company.
2. Amit Jaokar took over as Head of Technology at Motilal Oswal Financial Services in December. He was earlier CTO, Choice International.
3. Amitabh Mishra joined as President and Chief Technology Officer at Emcure Pharmaceuticals in July 2018. He was earlier with Vedanta Resources Ltd in its Sterlite Copper Division as its Chief Digital Officer.
4. Anjani Kumar took over a regional role as he joined as CIO, AMI (Africa, Middle East and India) for Nissan Motor Corporation in August. He was Senior VP and Global Chief Digital Officer of Collabera before that.
5. Annapurna Viswanathan joined as Head of Digital at Hindustan Coca-Cola Beverages in October. Immediately prior to this, she was IT Transformation Leader at GE Digital.
6. Anupam Singh took over as Head IT Jakson Group in April. He was earlier with Ericsson.
7. Asfar Khan was appointed as Director - Information Technology, South Asia of Kellogg Company in July. He served as CTO of Hindustan Coca-Cola Beverages immediately prior to this assignment.
8. Ashish Bajaj joined as Chief Technology Officer at DSP Mutual Fund in June. He was CTO at InstaRem, a Singapore-headquartered fintech.
9. Ashwin Prajapati joined Symphony Ltd as Group CIO in January 2018. He was a delivery director with KPIT Cummins Infosystems.
10. Bhavesh Lakhani joined SBI Mutual Funds as Senior Vice President and Head IT in May. He was the CTO of DSP BlackRock Mutual Fund before that.
11. Bhavin Purohit joined as the CTO of Tata Capital in June. He was CIO and Group IT Head of Welspun Group, immediately prior to that.
12. Biswabrata Chakravorty joined as the Chief Technology Officer of IndusInd Bank in February. He was earlier with Cigna TTK Health Insurance Company.
13. Chandresh Dedhia took over as Head of IT, Ascent Health & Wellness in January 2018 after a long seven-plus years term with Fermenta Biotech.
14. Chinmay Bhatia joined as Head IT at Reliance Nippon Life Insurance in November. Immediately prior to that, he was SVP and Head Business Applications with Liberty General Insurance.
15. CR Srinivasan was appointed as the Chief Digital Officer by Tata Communications in January 2018. He headed global cloud and security services business at the company. He would be responsible for technology, which was being handled by CIO Rupinder Goel, who retired.
16. Darshan Appayanna joined as Head Digital and Technology, Trent Hypermarket – Star Bazaar, a Tata & Tesco Enterprise in October. He was Chief Information & Knowledge Officer at Happest Minds prior to this.
17. Devendra Kumar Punia, an academician-turned-entrepreneuer-turned-corporate honcho, took over as CIO of Paras healthcare in July. He was the partner in two startups ProjectforSchool and Wunderkind.
18. Ekhlaque Bari was appointed as the Executive Vice President and CTO of Fullerton India in September 2018. He was earlier with Max Life Insurance for more than four years, immediately prior to this assignment.
19. Gautam Dutta joined as Chief Information & Technology Officer at Bajaj Allianz Life Insurance in November. He was VP, Technology with ICICI Lombard GIC.
20. Gupta Boda Head joined as IT & Digital of Brigade Group in April. He was Chief Technology Advisor to National Bank for Agriculture and Rural Development (NABARD) before that. He also served as CISO of GMR Group for a long time.
21. Harvinder Singh Banga was appointed as Chief Technology Officer at Samvardhana Motherson Group in July. He was Head of Business Application at GWC immediately prior to this appointment.
22. Madhavi Kanumoory took over as the CIO of Healthcare Global (HCG) in August. She was with GE Healthcare in various capacities for

> **In 2016 a number of CIOs changed the job they had held for more than five-six years. It accelerated in 2017. In 2018, this trend further diffused...**

These 'movers' are either joining a new company or taking a significantly different and bigger responsibility within the same company

more than five years prior to this assignment.

23. Mani Mulki joined as the Chief Information Officer at Tata Capital in June. Prior to that, he was with IFFCO based at UAE. He has also worked with ICICI Bank.

24. Maninder Karthik took over as Group CIO, Bottling Investment Group, The Coca-Cola Company in September. She was in Whirlpool Corporation for close to 8 years, in various positions, including CIO – Asia.

25. Manoj Kumar joined as Head - IT at APL Apolo Group (Apollo Pipes) in June. He was earlier heading IT function at Jakson Group.

26. Meheriar Patel joined Jeena & Company as Group CIO in April. He was CIO of AGC Networks immediately prior to that. He has also served in Sun Pharma.

27. Mohit Mendiratta joined as CIO V2 Retail in March. He was earlier with Havells India as General Manager - IT.

28. Nilesh Mhatre joined Bank of America India as its CIO in December. He was earlier with HSBC as its regional CIO for India.

29. Niranjan Balivade joined as Group CIO Eduspark Group in February. He was earlier with CEAT.

30. Pavan Tsunduru took over as CIO Great Eastern Shipping in December. He was earlier with Adani Ports and SEZ.

31. Priyabrata Sarangi joined as CIO, Eastman Auto and Power (Automotive division) in March. Before that, he served as the CIO of Exide Industries.

32. Puneet Kaur Kohli joined as CTO and CIO Manappuram Finance in January 2018 after spending more than four years as CIO of Bajaj Capital.

33. Rajesh Panchal, after a close to two-decade old stint at UPL, joined as CIO of Punjab Chemicals and Crop Protection in July.

34. Rajnish Sinha, who served as the Chief Digital Officer of Bajaj Electricals took over as the CIO of the company as well in August. This was following the retirement of Pratap Gharge.

35. Sandesh Govalkar joined as CIO and VP, ECL Finance in August. He was earlier Head of IT at Mirae Asset Capital Markets.

36. Sandip Kothari assumed the responsibility of CIO at Wonderchef Home Appliances. He has worked mostly with consumer and retail brands like Baggit, Travel Food Services, The Bombay Store, etc.

37. Sanjay Karnatak joined as the Chief Technology & Digital Officer at Star Union Dai-ich Life Insurance company in September. He was earlier with Aditya Birla Health Insurance.

38. Sanjay Kotha joined Ahmedabad-based conglomerate Adani Group as Joint President & Group CIO in January 2018. Immediately prior to that, he was serving as CIO & SVP at Hindustan Coca-Cola Beverages for close to five years.

39. Sanjay Verma joined as CIO of Somany Ceramics in November. He was earlier with JK Lakshmi Cements.

40. Sankarson Banerjee joined RBL Bank as the CIO in October. Before that, he was with National Stock Exchange as CTO – Projects.

41. Satya Saibaba Vakkalanka joined as Vice President IT and CIO at JMC Projects in October. He came from Turner Project Management India/Turner International where he served as Director – IS & Head of IT.

42. Shantanu Chatterjee took over as the Global Head - Digital IT at UPL in April. He was with Verizon Wireless in the United States for a long time.

43. Shrinath Bolloju was appointed as Managing Director, Operations & Technology and Head, Technology, South A by Citi in November. He was earlier COO at RBL Bank.

44. Shuvankar Pramanick joined as the CIO of Sir Ganga Ram Hospital at New Delhi in January. He was earlier Group CIO at Paras Healthcare

45. Subir Mookherji took over as Group CIO and Digital Business Leader at Solar Industries India in August. He was Vice President (IT) and head of Group IT CoE at RPG Enterprise.

46. Sudip Banerjee joined as Group CTO at Reliance Capital in March 2018. He moved from Reliance General Insurance where he had spent more than 10 years.

47. UC Singh joined as CIO, CEAT Ltd in March 2018. He left a more than seven-year stint with Greaves Cotton Ltd.

48. Veneeth Purushotaman joined as Group CIO at Aster DM Healthcare in September. He was CIO Fortis Healthcare before that.

49. Vipul Anand joined Hindware as SVP - IT in May. He had a more than four years-stint with Jindal Steel & Power before that.

50. Yoginder Grewal joined Hindustan Coca Cola Beverages as its CTO in July. He was with Sophie Paris in Indonesia■

Two Cybersecurity Risks Are Among Top Five Most Likely Global Risks For 2019

The World Economic Forum (WEF) *Global Risk Report* refers to Aadhaar breach, despite the Government's denial earlier

Two cyber security risks—data fraud/theft and cyberattacks—have been identified as the most likely risks for 2019 by the World Economic Forum (WEF), in its recently released annual *Global Risk Report (GRR)* for 2019. While extreme weather events, future of climate change mitigation and adaptation and natural disaster rank as the top three most likely global risks for 2019, data fraud/theft and cyberattacks follow at 4th and 5th most likely global risks for this year.

Both these risks figured among top five most likely global risks in 2018 too. WEF classifies the risks into five categories—Economic, Environmental, Geopolitical, Societal and Technological. It is significant that the five most likely risks are either environmental or technological.

The WEF GRR is based on its *Global Risk Perception Survey (GRPS)*.

The *WEF Global Risk Report* also ranks the risks in terms of impact. While none of the technological risks feature among the top five most impactful risks for 2019, two such risks feature among the top 10. Cyberattacks is the seventh most impactful risk, while critical information infrastructure breakdown features as the eighth most impactful risk. The risks that feature among the most impactful risks include weapons of mass destruction, extreme weather events, future of climate change mitigation & adaptation, natural disasters, water crises and bio-diversity loss and ecosystem collapse feature as the most impactful risks.

Four technological risks have been identified by the GRR as top global risks. Apart from data theft/fraud, cyberattacks, and breakdown of critical information infrastructure, adverse consequences of technological advances too figure as one of the top global risks, albeit towards the bottom of table. Data fraud/theft also figures somewhat lower in the list of risks when it comes to impact, even though it features as one of the fourth most likely global risks.

Breakdown of critical information infrastructure featured as one of the top five most impactful risks in 2014 but since then, no other technological risks have featured in the list of top five most impactful risks.

Dissecting technological risks

According to the GRR 2019, a large majority of respondents expected increased risks in 2019 of cyberattacks leading to theft of money and data (82%) and disruption of operations (80%).

Around two-thirds of respondents expect the risks associated with fake news and identity theft to increase in 2019, while three-fifths said the same about loss of privacy to companies and governments.

"Cyber vulnerabilities can come from unexpected directions, as shown in 2018 by the Meltdown and Spectre threats, which involved weaknesses in computer hardware rather than software. They potentially affected every Intel processor produced in the last 10 years," said the report.

"Last year also saw continuing evidence that cyberattacks pose risks to critical infrastructure. In July the US government stated that hackers had gained access to the control rooms of US utility companies. The potential vulnerability of critical technological infrastructure has increasingly become a national security concern," it added.

The report said the second most frequently cited risk interconnection in this year's GRPS was the pairing of cyberattacks with critical information infrastructure breakdown.

"Machine learning or artificial intelligence (AI) is becoming more sophisticated and prevalent, with growing potential to amplify existing risks or create new ones, particularly as the Internet of Things connects billions of devices," it notes quoting research by IBM and others published earlier.

Among the most widespread and disruptive impacts of AI in recent years has been its role in the rise of "media echo chambers and fake news", a risk that 69% of GRPS respondents expect to increase in 2019, the report said. Researchers last year studied the trajectories of 126,000 tweets and found that those containing fake news consistently outperformed those containing true information, on average reaching 1,500 people six times more quickly. One possible reason cited by researchers is that fake news tends to evoke potent emotions: "Fake tweets tended to elicit words associated with surprise and disgust, while accurate tweets summoned words associated with sadness and trust." The interplay between emotions and technology is likely to become an ever more disruptive force, the report notes.

According to the GRR 2019, a large majority of respondents expected increased risks in 2019 of cyberattacks

Aadhaar breach

Interestingly, the GRR unequivocally refers to the Aadhaar data breach, reported widely last year but later denied by the government.

"Malicious cyberattacks and lax cybersecurity protocols again led to massive breaches of personal information in 2018. The largest was in India, where the government ID database, Aadhaar, reportedly suffered multiple breaches that potentially compromised the records of all 1.1 billion registered citizens," the report says.

"It was reported in January that criminals were selling access to the database at a rate of INR 500 for 10 minutes, while in March a leak at a state-owned utility company allowed anyone to download names and ID numbers," it says quoting BBC and ZDnet reports.

In October last year, after a similar report by security vendor Gemalto's popular *Breach Level Index*, the Government got into a denial mode and the vendor had to retract its claim and apologize.

It remains to be seen how the Indian Government reacts to the observation made by the World Economic Forum's report.■

Blockchain Can Transform World Trade But Challenges Remain: WTO Report

The report identifies specific opportunities—and challenges too

Even as enterprises wake up to the potential of Blockchain, a new report by World Trade Organization (WTO) has identified how the trending technology can revolutionize world trade.

The publication, *Can Blockchain revolutionize international trade?* explores how exactly can the technology enhance trade and what challenges need to be tackled before the potential of Blockchain can be fully realized.

Some of the potential impact that the WTO report has identified are as follows:

Blockchain could help trade move closer to becoming paperless.

The report says Blockchain could enhance efficiency of trade processes and achieve truly paperless trade, subject to removal of certain obstacles.

"The intrinsic characteristics of the technology also make it a potentially interesting tool to help implement the WTO Trade Facilitation Agreement (TFA) and to facilitate business-to-government (B2G) and government-to-government (G2G) processes at the national level. Blockchain and smart contracts could help administer border procedures and national single windows (a single point of entry through which trade stakeholders can submit documentation and other information to complete customs procedures) in a more efficient, transparent and secure manner, and improve the accuracy of trade data," it notes.

Blockchain could give rise to a new generation of services.

The multilateral organization sees Blockchain facilitating introduction of new services in areas like financial services, e-commerce and insurance, terming it, "the infrastructure of the services industry." "Blockchain could be to the services sector what robots have been to manufacturing," the report says.

Blockchain could help administer intellectual property (IP) rights in a more efficient and transparent way, and help fight counterfeits.

The report observes that Blockchain applications could impact both the governance of IP rights and the IP industry itself. "Blockchain for registered and unregistered rights could arguably be used to provide proof of creation, existence, ownership and/or first use, to register IP rights, to facilitate the administration and management of IP rights on a global scale, thereby potentially contributing to the emergence of "global IP chains", and to enforce IP rights and fight counterfeits in a more efficient way," it notes while identifying challenges that need to e tackled before this could be realized.

Blockchain could enhance government procurement processes.

The report say Blockchain holds promises for government procurement processes, manage public contracts more efficiently, and fight fraud, but t is essential to weigh the costs and benefits carefully.

Blockchain could help build trust and enhance the transparency of supply chains.

The report also reiterates raison d'être of Blockchain in the business world – its potential to build trust and enhance transparency of supply chains. It can impact trade significantly.

Blockchain has the potential to reduce a variety of trade costs substantially.

All the above could reduce trade cost significantly, says the report, quoting World Economic Forum (WEF) estimates that that removal of barriers due to Blockchain could result in more than USD 1 trillion of new trade in the next decade.

Blockchain opens up new opportunities for micro, small and medium- sized enterprises (MSMEs) and small producers from developing countries.

The report also recognizes Blockchain's potential to better participation of MSMEs in international trade, by facilitating access to trade finance, facilitating trade procedures, and reducing trade costs—thus removing many barriers that exist.

However, the potential can be realized only when certain challenges are met, the report says unequivocally.

The report lists several technical challenges such as:

- **Scalability**
- **Security**
- **Interoperability** because of numerous platforms using different technical interfaces and algorithms which do not "talk to each other".
- **Standardization (lack of it) of the information exchanged** (International organizations, such as the International Chamber of Commerce (ICC), International Organization for Standardization (ISO), United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) and the World Customs Organization (WCO), have created working groups to initiate discussions to look into the issue and develop interoperability standards.)

Among the legal issues, the WTO report points to:

- **Lack of conducive regulatory framework** that recognizes the legal validity of blockchain transactions, clarifies applicable law and liabilities, and regulates the way data can be accessed and used. The most critical issue relates to the legal status of blockchain transactions.
- **The recent legislations around data privacy** The report says the codification of law that aims at making laws machine-readable is a requirement in order to facilitate the transposition of contractual obligations into digital contract code (smart contracts), and the development of a global legal identification of companies.

The publication calls for a multi-stakeholder dialogue to assess the practical and legal implications of the technology and to develop collective solutions to existing challenges while providing the flexibility for the technology to thrive.

"While this technology opens interesting opportunities, clearly it also raises legal, regulatory and policy issues that deserve our attention. We need to consider how to spread the opportunities and overcome the challenges. We can only do this if we are in full possession of the facts. We need to fully understand the technology – what it can do and what it can't do. And most importantly for us, we need to understand what it means for international trade," said WTO Director-General Roberto Azevêdo.

"This requires an informed debate. And it needs to go beyond trade experts. Blockchain is a technology that has the potential to break silos, so we should not create silos in this discussion. We need a debate among all stakeholders – the business community, blockchain experts, government authorities, representatives from other international organizations, and many others as well. With our new publication, and with today's event, we are seeking to inform the debate and bring together this wider community," he said■

Key Tech Trends That Will Dominate The Retail Sector In 2019

Quantum computing is one of the key tech trends

In today's modern retail environment, information is available everywhere. Consumers are well informed and expect personalized experiences when they shop. This means that the table stakes have changed – retailers now need an IT strategy that expands well beyond a web presence into all areas of their business. Fortunately for retailers, technological innovations across cloud computing, data analytics and AI are enabling a new era, where it's possible to gain ten times the insights in one-tenth the time. Retailers that embrace these technologies are well positioned to not only lead their industries, but also take share from the laggards.

In the backdrop of this, as per Microsoft, there are 5 technology trends that will dominate the retail sector in 2019:

1. More AI-powered retail applications will gain adoption as the technology matures: Retailers are already utilizing AI to deliver a highly personalized experience. High-end retailers are using AI powered devices to increase their knowledge of customers to deliver better products and services. By employing types of AI like machine learning, companies can begin to anticipate customers' requests and desires, positioning themselves to build a stronger relationship by tailoring offers and interactions to each specific customer. AI and machine learning can also play a significant role in helping retailers optimize their supply chain. The retailers are also using Artificial Intelligence to leverage the benefits of voice assistants like Cortona, Alexa, Facebook Messenger, etc. By 2019, about 40% of retailers will develop a customer experience architecture supported by AI, boosting conversions up to 30% and revenue by 25% through hyper-micro personalization.

2. Voice Technology: Voice assistants can prove to be a game changer in the retail industry in the year 2019. Voice technology integrated with AI helps consumers discover products faster, hence changing our shopping behavior. With the push for 5G connectivity, number of connected devices and connected people will rapidly grow which in turn will support the growth of voice commerce. Voice commerce will help customers in browsing and choosing products with the help of voice assistants present in the market today. Merchants will have the opportunity to put themselves on the radars of target customers. The retailers who have set up a proper online listing and optimized their site local search will stand a good chance of being recommended to the customer.

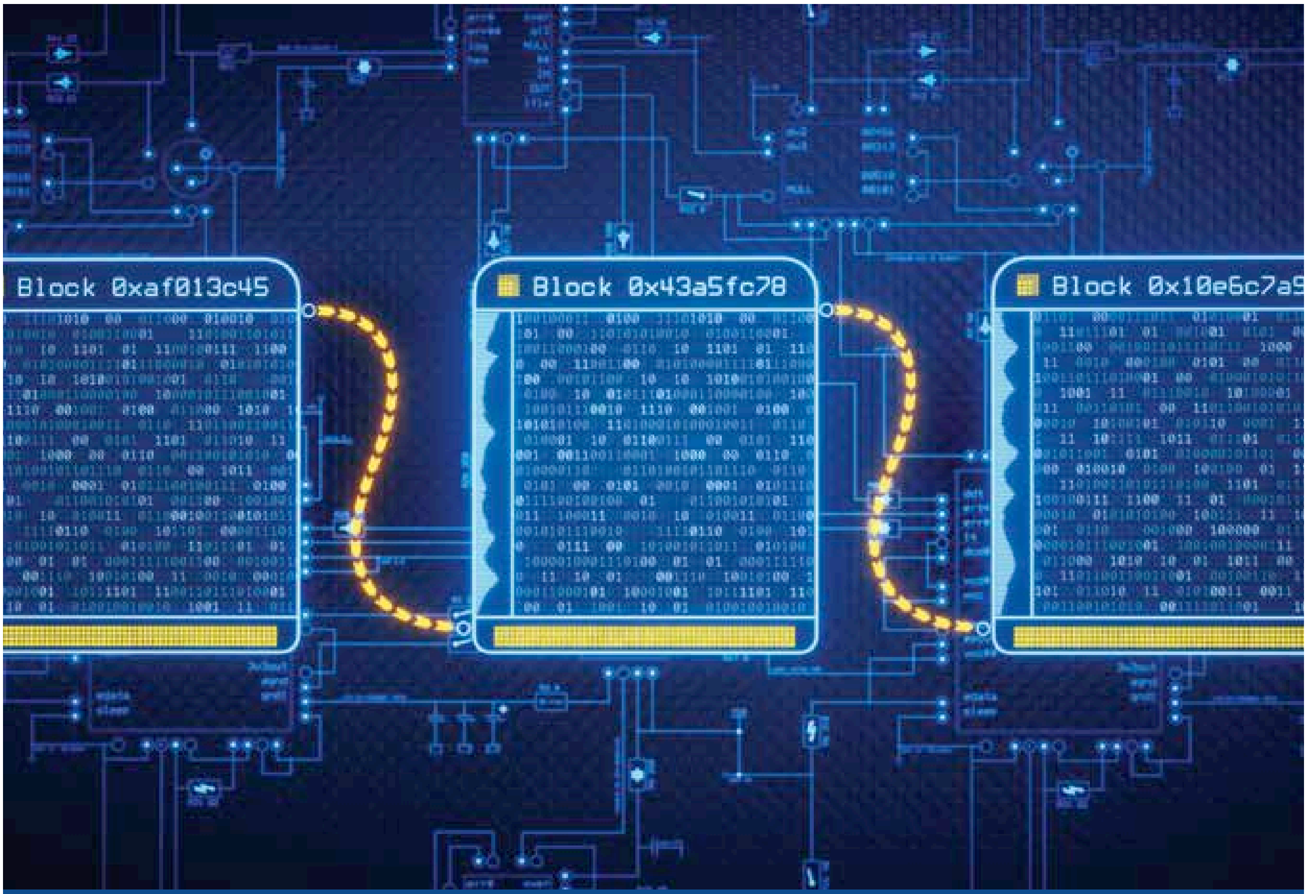
3. Internet of Things: The internet of things has already gained momentum in the year 2018, however in 2019 the technology will move beyond the hype cycle-enabling retailers to turn possibility into reality. Many retailers have already launched pilots for their stores as they view IoT as a backbone of data-driven economy. The data collected through various IoT devices can be used to study the consumer behavior and preferences. The technology has the potential of taking personalization in retail to a whole new level. IoT along with machine learning models and data visualization can create differentiated and highly personable experiences and products. For example, Nordstrom Rack is using in-store beacon technology from Footmarks, built on the Microsoft Cloud, to better engage and personalize shoppers' experiences and ultimately increase speed and convenience.

4. Virtual Reality & Augmented Reality: The adoption of Virtual Reality and Augmented Reality in retail is reshaping buyer behavior and the shopping journey. The technology promises an enhanced shopping experience. In 2018, VR & AR was focused on in-store experience, however in 2019 the application of the technology will also focus on e-commerce. The technology is not just limited to the ability to put buyers in the virtual world and try out products via VR and AR powered devices, but it can also help the retailers come up with innovative products and retail spaces. The future of AR and VR in the retail sector will have two major use cases:

- With the use of AR and VR powered devices, a customer can see how the product will look in his house. For example, a customer can see how a piece of art or furniture will look in his house – hence, providing a better shopping experience.
- On the other hand, the technology can be very helpful in store designs and shelf layout. A VR-generated store will let the shoppers browse the virtual space from anywhere.

5. Quantum Computing: In the future, Quantum computing will remould our economic, industrial, academic, and societal landscape. A quantum computer can cater to complex problems that today's computer will take millions of years to solve, in just hours or days. Most likely quantum computing will augment subroutines of classical algorithms which can be processed on quantum computers to tackle specific challenges faced by the retail sector. Also, retail sector generates huge amount of data which is analyzed to study shoppers' demographics & preferences and manage the supply chains efficiently. With the introduction of quantum computers, the process of analyzing the data will become much faster and easier- hence making it easy to deliver highly personalized experience to the customers. Microsoft envisions a future where quantum computing is available to a broad audience, scaling as needed to solve some of the world's toughest challenges. The quantum approach begins within familiar tools we know and use such as Visual Studio. It provides development resources to build and simulate quantum solutions, and it continues with deployment through Azure for a streamlined combination of both quantum and classical processing■

> Retailers need an IT strategy that expands well beyond a web presence into all areas of their business. Fortunately, technological innovations are enabling a new era...



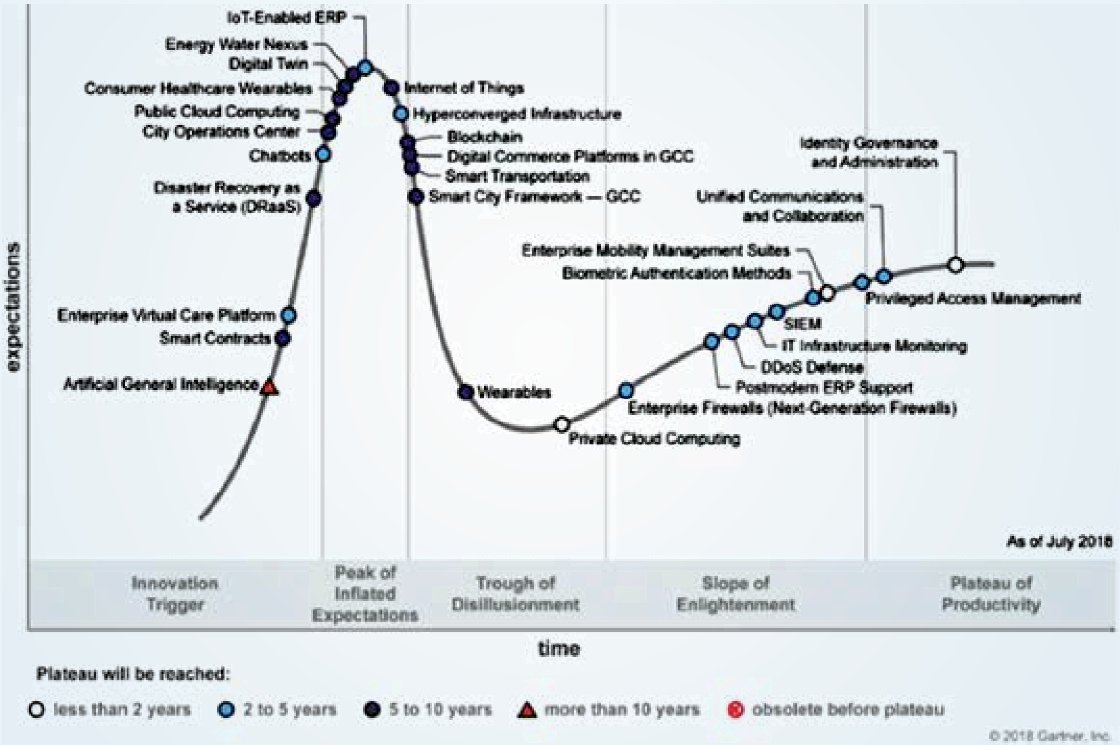
Key Technologies That Will Reach Mainstream Adoption In Five To Ten Years

Digital twins and smart contracts feature among them

Blockchain, IoT, city operations centers, smart city frameworks, digital twins and smart contracts are among the technologies that will achieve mainstream business adoption in the next five to 10 years, according to Gartner.

Of the 29 technologies on this year's Gartner's *Hype Cycle for IT*, eight are entering the Slope of Enlightenment and climbing toward the Plateau of Productivity (see Figure 1).

Figure 1: Gartner's 2018 Hype Cycle for IT



Source: Gartner (December 2018)

Although blockchain technology maintains high visibility, Gartner does not expect blockchain architectures to be suitable for many enterprise activities, especially taking account of issues of decentralization, risk and governance. However, startups may continue to seek disruptive opportunities using the original block and chain concept, and Gartner recommends that business executives undertake scenario planning accordingly.

CIOs considering implementing blockchain technology should use clear language and definitions in internal discussions about the nature of this technology. They should also identify the points of integration with their existing infrastructures (such as digital wallets and core systems of record) to help determine future investment plans.

IoT has a business transformation and evolutionary impact on most organizations as it can be used as a key enabler to deliver services and create new business opportunities.

CIOs considering implementing blockchain technology should use clear language and definitions in internal discussions about the nature of this technology and identify the points of integration...

IoT projects will impact most organizations' competitive position, product development strategy and internal operations, as connected things will help generate revenue and lower costs.

A digital twin is a virtual representation of a real object that is designed to optimize the operation of assets such as aircraft, power plants and buildings. The primary short-term use is to lower maintenance costs and increase asset uptime.

Organizations considering the use of digital twins should focus on identifying a portfolio of digital twin initiatives that provide short (within one year) and midrange (within five years) paybacks. Simultaneously, they need to conduct a threat and opportunity analysis of their current business ecosystem, incorporating digital twin developments by competitors or partners■

Edge Will Drive Change In 2019: Study

The Vertiv study identifies top five 2019 datacenter trends

The edge of the network continues to be the epicenter of innovation in the datacenter space as the calendar turns to 2019, with activity focusing on increased intelligence designed to simplify operations, enable remote management and service, and bridge a widening skills gap, according to a study by Vertiv. This increasing sophistication of the edge is among the datacenter trends to watch in 2019 as identified by Vertiv experts from around the globe.

"Today's edge plays a critical role in data center and network operation and in the delivery of important consumer services," said Vertiv CEO Rob Johnson. "This is a dramatic and fundamental change to the way we think about computing and data management. It should come as no surprise that activity in the data center space in 2019 will be focused squarely on innovation at the edge."

1. Simplifying the Edge: A smarter, simpler, more self-sufficient edge of the network is converging with broader industry and consumer trends, including the Internet of Things (IoT) and the looming rollout of 5G networks, to drive powerful, low-latency computing closer to the end-user.

For many businesses, the edge has become the most mission critical part of their digital ecosystem. Intelligent infrastructure systems with machine learning capabilities working in tandem with cloud-based analytics are fundamentally changing the way we think about edge computing and edge services. The result will be a more robust, efficient edge of the network with enhanced visibility and self-healing capabilities requiring limited active management.

Sharing views on the edge trend, Sunil Khanna, president and managing director at Vertiv, India, said, "Most industries in India are recognizing the limitations of supporting users and emerging technologies through centralized IT infrastructures and are pushing storage and computing closer to users and devices. That shift is becoming necessary because of the increased connectivity of devices and people and the huge volumes of data they generate and consume. We believe this will require profound changes in the compute and storage infrastructure to support the smart and connected future, particularly at the local level."

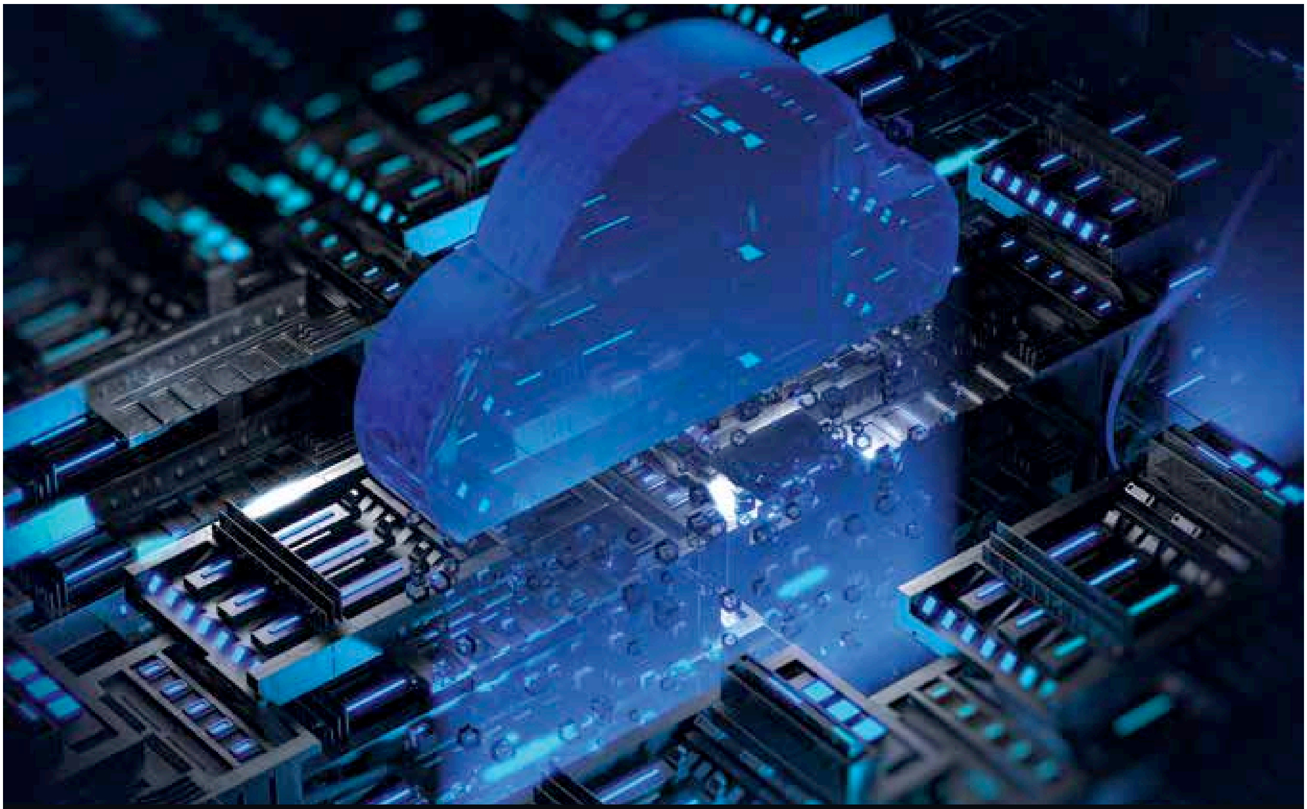
2. Workforce Revolution: A workforce aging into retirement and training programs lagging behind the datacenter and edge evolution are creating staffing challenges for datacenters around the globe. This will trigger parallel actions in 2019. First, organizations will begin to change the way they hire datacenter personnel, moving away from traditional training programs toward more agile, job-specific instruction with an eye toward the edge. More training will happen in-house. And second, businesses will turn to intelligent systems and machine learning to simplify operations, preserve institutional knowledge, and enable more predictive and efficient service and maintenance.

For many businesses, the edge has become the most mission critical part of their digital ecosystem. Intelligent infrastructure systems with machine learning capabilities working in tandem with cloud-based analytics are fundamentally changing the way we think about edge computing and edge services

3. Smarter, More Efficient UPS Systems: New battery alternatives will present opportunities for the broad adoption of UPS systems capable of more elegant interactions with the grid. In the short term, this will manifest in load management and peak shaving features. Eventually, we will see organizations using some of the stored energy in their UPS systems to help the utility operate the electric grid. The static storage of all of that energy has long been seen as a revenue-generator waiting to happen. We are moving closer to mainstream applications.

4. Pursuing Normalization: The datacenter, even in the age of modular and prefabricated design, remains far too complex to expect full-fledged standardization of equipment. However, there is interest on two fronts: Standardization of equipment components and normalization across datacenter builds. The latter is manifesting in the use of consistent architectures and equipment types, with regional differences, to keep systems simple and costs down. In both cases, the goal is to reduce equipment costs, shorten delivery and deployment timelines, and simplify service and maintenance.

5. High-Power Processors and Advanced Cooling: As processor utilization rates increase to run advanced applications such as facial recognition or advanced data analytics, high-power processors create a need for innovative approaches to thermal management. Direct liquid cooling at the chip – meaning the processor or other components are partially or fully immersed in a liquid for heat dissipation – is becoming a viable solution. Although most commonly used in high-performance computing configurations, the benefits – including better server performance, improved efficacy in high densities, and reduced cooling costs – justify additional consideration. Another area of innovation in thermal management is extreme water-free cooling, which is an increasingly popular alternative to traditional chilled water■



India To Lead the World In Hybrid Cloud Adoption: Study

The Nutanix study reveals the adoption of hybrid cloud workloads in India will more than triple from 13% today to 43% in the coming 24 months

India is set to lead the world in hybrid cloud usage and adoption over the next two years, according to a new global study by Nutanix.

The report, "The Nutanix Enterprise Cloud Index" compiled by Vanson Bourne, and commissioned by Nutanix found the adoption of hybrid cloud workloads in India will more than triple from 13% today to 43% in the coming twenty-four months.

This rapid adoption is likely to help boost India's economic muscle as the economy reaps the benefits from enhanced productivity and efficiency, while the nation's enterprises become more flexible and resilient. As Asia redefines its landscape in the light of the rapid onslaught of digital transformation – those nations equipped to maximize the potential from a fully connected economy will have a considerable advantage.

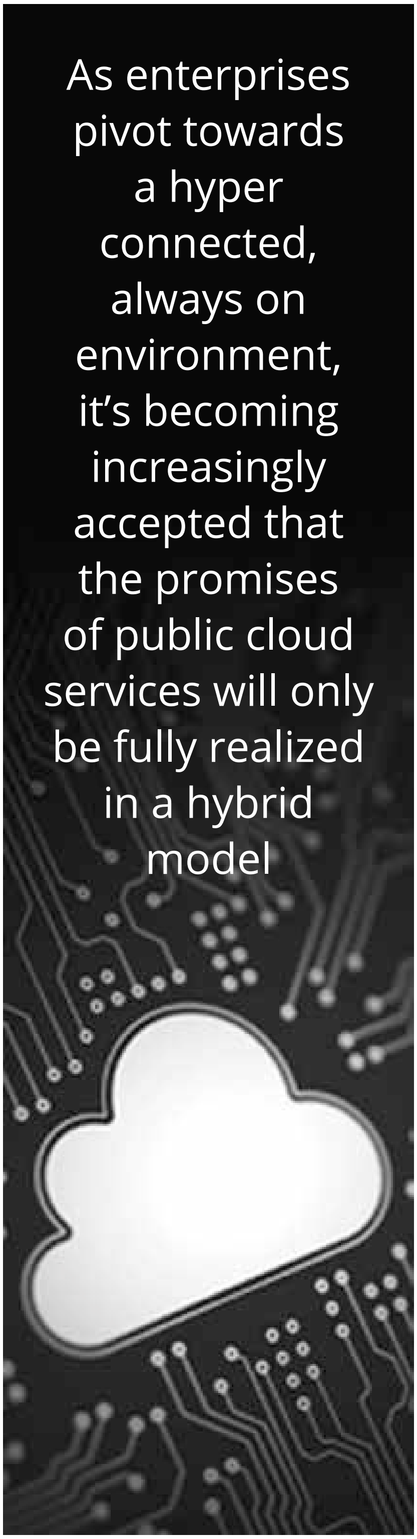
As enterprises pivot towards a hyper connected, always on, and digital environment, it's becoming increasingly accepted that the promises of public cloud services will only be fully realized in a hybrid model – where public and private cloud environments of any type and size are fully integrated and interoperable.

This is where hybrid can add true value, providing enterprises with benefits, such as greater workload flexibility, simplicity in processing big data, broader use of cross platform IT services, enhanced data security and compliance, dramatic cost reduction and greater business growth and RoI.

The report is Nutanix's first annual index aimed at measuring the global state and adoption of traditional and next generation private, public and hybrid cloud, including Indian enterprises.

The study identifies cloud experiences, priorities and trends of Indian enterprises and how they compare globally and in Asia Pacific and Japan (APJ) region. The research found that India respondents use of private cloud ranked high and was surpassed only by Italy (49%), Germany (43%) and France (39%); however, the country trailed most of its global peers in hybrid cloud deployments with just 13% penetration, marginally ahead of France (11%) and the Nordics and the Netherlands with 12% respectively.

For India, the research suggests 91% of respondents agree cloud computing has increased the efficiency of their IT departments, 81% opine that mobility of applications between cloud environments is essential and 61% believe that having a simple way to move workloads from cloud to cloud and from cloud to on-premise infrastructure will solve a lot of problems.



As enterprises pivot towards a hyper connected, always on environment, it's becoming increasingly accepted that the promises of public cloud services will only be fully realized in a hybrid model

Below are other key India findings of the report:

Further investments on time, money and skills on cloud services

Study findings reveal that India will convert much of its private cloud usage (38%) to hybrid usage, as its use of private clouds is expected to drop by about a third (23%) during the same period it expects its hybrid use to more than triple (43%).

While business and data security are key priorities, IT performance is a major benefit

Data security and compliance were ranked as the single biggest benefit of using a public cloud, on average, globally. These attributes tied with lower total cost of ownership (TCO) as the top perk when ranked by enterprises in the APJ region. India showed a higher ranking of security as a benefit than the global and APJ averages; however, it placed an even higher emphasis on performance, which it ranked as the number one public cloud benefit.

India also seemed to value agility, scalability, and cost reduction less—and ease of management more—than its regional and global counterparts.

Indian enterprises seem to fare better in controlling public cloud spend

While public cloud service deployments were reported to exceed IT budgets by 36% of both global and APJ respondents, only 23% of Indian respondents reported being over budget with their public cloud services; 77% reported being on or under budget.

Indian companies are doing better in getting all needs met by public cloud services

More than half of Indian respondents (54%) indicate that all their needs are being met by public cloud services —12% higher than the global average and 22% higher than the average in the APJ region■

Key Trends That Will Drive IT Transformation In 2019

Automation transforming the workforce will be one of the trends

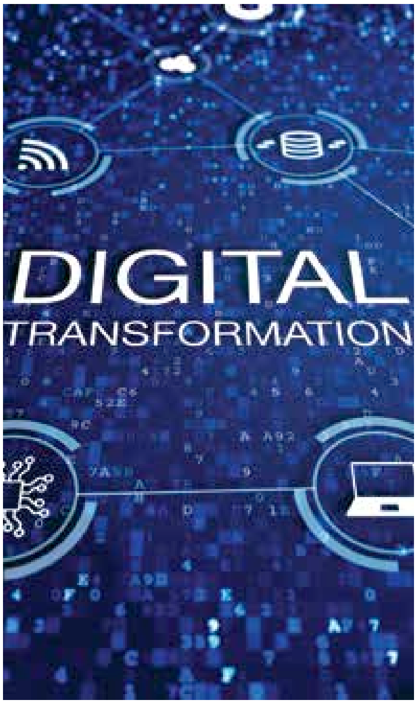
Enabling the business outcome in a 'real-time' enterprise environment is the next challenge for global brands and government agencies in 2019. Tech companies will need to drive hard to continually exceed to their customers' expectations during a time of accelerating change. They will need to show how technology can help deliver on their customers' objectives, improve agility, security and impact, or they risk being disrupted.

Here is Verizon Enterprise Solution's view of those enterprise technology trends that are most likely to impact our global business and government customers in 2019:

1. The real-time enterprise will begin to transform how business works: Foundational technologies – Software-defined Networks, 4G, the Internet of Things, intelligent video, security, telematics - are already changing the operations of business. In 2019, savvy CIOs will be focusing on how to reinvent their operations to leverage the enormous potential promised by disruptive technologies like 5G, artificial intelligence/machine learning, automation and robotics, augmented and virtual realityand the next-gen cloud including edge computing. Many of these technologies have now moved from concept to reality, and those who can best leverage the advantages they bring will increasingly be well placed to win the future.

2. Businesses will invest for performance: CIOs are recognizing that the network they use really matters to their business –a secure, strong network foundation enables them to deliver innovative platforms and solutions that will move their business forwards. Then, it's all about the service model and the tech surround that makes network-reliant applications available - the support, the professional services, service level agreements and more. The key is to find an expert partner with the network expertise to help you deliver on your business objectives. You can't run a modern business without secure network capacity.

3. We'll remember that the customer is king: Customer experience (CX) has been a hot topic over recent years, but many of us have had personal experience of the big brands letting us down. With AI infiltrating CX systems, there's an unprecedented opportunity to move to a principle of 'personalization for you', putting the customer back in the center of the business opportunity. The best organizations will use data to inform human engagement, remembering that this is what creates real relationships. But they'll leverage technology to do this at speed and scale.



CIOs are recognizing that the network they use really matters to their business – a secure, strong network foundation enables them to deliver innovative platforms and solutions

4. We'll focus on the transaction guarantee: We've talked about Software-defined Networking (SDN) for a while, but it's now out there, live, and transforming business opportunities all around the globe, configured to match your cost and security requirements. In 2019, organizational success will be driven by how well CIOs leverage the many options that SDN enables, delivering agility, flexibility, and scale to run their business. It's now beyond application-aware networking, and instead, about focusing on the transaction guarantee, and defining policies to support the specific application, time or location needs that will make the difference.

5. Contextual privacy will be front and center: There's never been a bigger focus on the importance of privacy, as data breaches continue to hit the headlines. Application users are keenly interested in how their data is used. In 2019, we'll begin to see a focus on contextual privacy requirements, linked to location-based awareness. This will change how organizations are able to approach their security, and keep personal data safe.

6. Automation will transform the workforce: Robotic process automation and machine learning will transform how business operates – and what skills a business workforce needs. In 2019, educators and businesses will focus on how to build a pool of data scientists and ML specialists to support our future skills needs, rather than yesterday's business requirements.

7. We'll go back to basics on security (again), but also focus on specifics: In 2019, organizations will redouble their efforts to strengthen their security posture. It's about understanding their risk environment, and ensuring they are doing the basics right to protect their business;practicing IT hygiene to keep infrastructure current to protect against vulnerabilities continues to be critical. Network-level security is essential – in a software-defined world, network segmentation and security is a central part of the design. But they'll also increasingly need visibility on data to drive insights and ultimately decisions on how to mitigate against specific security threats. But action will be taken – or the board or the customer will ask why■

Double Scoop

Two times
the revelation

Santosh Mankar

Associate Vice President - IT
SBI Life Insurance Co

A SPORTS PERSON I IDOLIZE

Kapil Dev

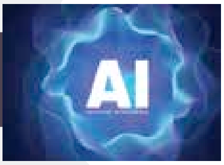
MY FAVORITE DRESS

Business Formals

MY FAVORITE TECH MAGAZINE

Express Computer

AN EMERGING TECH THAT'LL HAVE THE MAXIMUM IMPACT IN 2019



AI

MY FAVORITE HOBBY

Travelling to unknown places

MY PEER IN THE IT COMMUNITY

Atul Shirwadkar

Support Manager - IT, Nucsoft

MY FAVORITE GADGET

Smartphone

MY FAVORITE GETAWAY

United Kingdom

A TECH IDOL I WOULD LIKE TO MEET

Satya Nadella

MY FAVORITE CUISINE

Paneer Bhurji

A TECH SHOW I LOVED WATCHING

4D Tech Show

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