Opinion | Pg 20
Artificial Intelligence: Changing Healthcare Landscape

Insight | Pg 26
Securing SWIFT Environment Within Banks

ITNEXT

FOR THE NEXT GENERATION OF CIOs

NEXT100 2019
APPLICATION OPEN
see Page 37 for details

THE CIO'S ROLE: AS THE NexGen SEES IT

More than 40 NEXT100 winners share how they see a CIO's role

May 2019 | ₹100 | Volume 09 | Issue 12 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

WHO CAN APPLY?

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

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

WHY APPLY?

By participating in the NEXT100 process you get:

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

HOW TO APPLY?

To get started with the NEXT100 application process:

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

APPLICATION OPEN
20TH MAY

APPLICATION CLOSE
1ST JULY

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

INDIA's FUTURE CIOs
NEXT 100
2019

10 years
2010-2019

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

Is agility the way out?

"Agile planning, despite being used extensively in IT project management, has not really been employed in overall technology management because of the nature of capex planning. But with cloud, that handicap is removed and there is far more flexibility"

Shyamanuja Das

In the cover story of this issue, we explore a sensitive, if not difficult, topic—what the NexGen IT managers think the CIO role should be. As I have written in the story, there is both good news and bad news. Good news is that they talk of the same issues, same challenges and use the same language as the CIOs do.

As I have argued, this could be seen as bad news too. The next-in-line does not see things too differently. We need change for progress.

Today, things are changing so fast that it is difficult to believe that what is considered great practice today will be effective in three years. So, how can we expect the current next-in-line to achieve results tomorrow by adhering to today's thoughts?

You do not need an expert to tell you they will not.

However, look at the other side of the coin. Things are changing so fast that unless you understand it completely—that is almost impossible—and can influence its direction significantly—not too many of them can—it is difficult to plan something drastically different. Maybe, they are sensitized to this but are playing safe.

Maybe, they want to take things as they come.

That is not a bad idea. But it cannot be done in a passive manner. You may not plan for too distant future but you need to have a way of working, a model that allows you to factor in changes continuously.

Thankfully, that model exists and IT guys are only too familiar with it. They call it agile methodology and that is used extensively in IT projects. Can that be adopted in technology management per se?

The thought is not new. It has been proposed earlier. And many of the same IT managers do follow it when it comes to managing large technology projects. But few do it that way for the entire technology management.

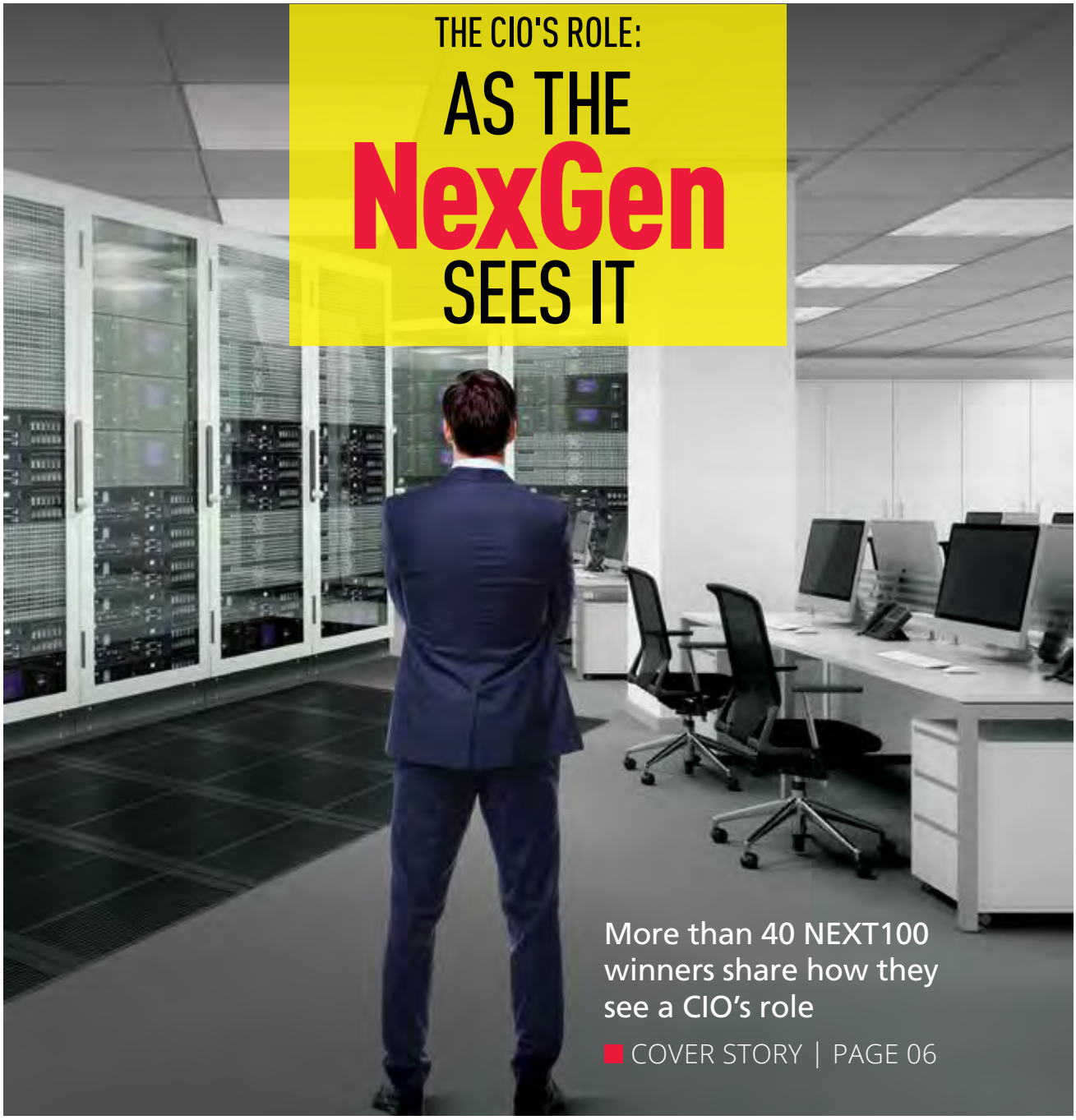
There was a reason for it. Typically, capex planning happens in spurts and rollout takes time. So, real agile planning was not possible.

But with cloud becoming mainstream enterprise platform, that would no longer be an issue.

Will the next generation CIOs go for agility in entire tech management a far more focused manner? ■

MAY 2019
VOLUME 09 | ISSUE 12

Content



THE CIO'S ROLE: AS THE NexGen SEES IT

More than 40 NEXT100 winners share how they see a CIO's role

COVER STORY | PAGE 06

Cover Design:
ANIL VK

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

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

EDITORIAL
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
Assistant Brand Manager - Enterprise Technology: 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
Manager - Events: Himanshu Kumar
Manager - Events: Naveen Kumar

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

Editor: Vikas Gupta

99 GROUP

EXTRA Curricular

Life's moments in frame for eternity

Through The Lens...

NEXT100 Winner 2017 **Sohil Laad,** ERP/SAP Operations & Technology Lead, Syngenta shares his passion for photography and travelling...

Photography is my passion. I am a simple man who loves taking photographs and spending time with my family. All this started as a short-sighted journey of a gadget nice-to-have to a hobby that I follow from my heart. I give the entire credit to my wife, who motivated me to pursue this passion. Landscapes, macro, nature and travel inspire me. In short, I love photography because it captures moments forever, which are long gone! I caught the photography virus at the age of eighteen. I was a gadget freak and wanted to buy a SLR camera. I started taking photos with that camera. It was post my marriage that my wife saw my photos and asked me to pursue this as a serious hobby. I took a brief one week course to understand the basics and then went ahead full throttle. I started following the photographs of great maestros like Ansel Adams, Raghu Rai, Hokkaido, et. al., to learn from them. I started taking my camera whenever possible even when I went around my city (Pune).

I love travelling and, of course, I take my camera along and explore the world through my lens. While I have mostly travelled within Europe, through Syngenta (my current company), I got a chance to visit South East Asia – Singapore. This was my latest visit where I spent a lot of time capturing the night life and skyline. This hobby also helped me connect with several similar interest groups and take part in contests. I learnt a lot and that helped me boost my passion. These connects also exposed me to various events and competitions and guided me on how your passion can be shared with the world. My photos were selected for Lonely Planet magazine and on the 2016 Bausch + Lomb calendar!

Finally, one attitude I always practice is "Boldly Go Where No Man Has Gone Before", which is basically experimenting and BREAK ALL RULES! ■

As told to Dipanjan Mitra, Team ITNEXT

Sohil Laad

Snapshot

Sohil Laad is ERP/SAP Operations & Technology Lead at Syngenta. He is NEXT100 Winner 2017. In the past, he has worked in various managerial and leadership capacities in companies like Wipro and Cognizant. He has done his Bachelors in Computer Science.

On A Musical Journey...

NEXT100 Winner 2017 **Subhanil Banerjee,** Senior Manager – IT Infrastructure & Security, ABP shares how his passion for music keeps him going strong

Music boosts your brain power and makes you feel relaxed. There are many types of music. Some people like to listen to rock music and some others like pop music. Music is a really good way to reduce stress by relaxing your mind.

Listening to music is not just a hobby but a passion that can never tire the soul of the music lover. Rhythm is the core of music that actually stimulates your brainwaves and heartbeats into a happy state. At times even if the lyrics slip out of your mind, the melody lingers beautifully in the memory of the music lover. If variety is the spice of life; music is all spiced up in variety as it has classical, pop, rock, hip hop, you name it, and you get it. Music breaks barriers as any good song, irrespective of the language, can be heard if the music is good. Plain instrumental music is actually a wordless delight that speaks the mellifluous language of the soul. It is emotive, approachable and can be personalized to suit your moods and persona. Use it as a creative input or as the expression of your many moods and emotions.

I personally have been inspired by legendary musicians Mozart, Beethoven, Elvis and Beatles. There is no such thing as "best" in art, objectively; though you frequently hear that Beethoven's symphonies with odd numbers are the best. My preference is as follows: 7th, 5th, 3rd and 6th.

Indian music takes many forms: classical, folk, and pop music. India has been blessed with a number of gifted musicians, who have mesmerized listeners from around the globe. I'm no exception. My favorite is R.D. Burman, popularly known as 'Panchamda'. He was the man who introduced Western tunes in the Hindi film industry. His musical ideas were innovative and fresh to Indian ears. Heavily inspired by Western music, especially Arabian and Persian music, he experimented with several genres to create fusion music and some boundary-breaking songs. Some of my all-time favorite R.D. Burman compositions are:

1. *Tere bina zindagi se koi* from Aandhi
2. *Kya yahi pyar hai* from Rocky
3. *Chura liya h tumne* from Yaadon Ki Baraat
4. *Do lafzon ki hai dil ki kahani* from The Great Gambler
5. *Zindagi ke safar me* from Aap Ki Kasam
6. *Tujhse naraz nahi zindagi* from Masoom
7. *Kya hua tera wada* from Yaadon Ki Baraat

My first instrument is the piano. My grandfather had one and from a young age, I would try to play it. Eventually, my dad got an electronic keyboard. I played with it a lot, even teaching myself some songs.

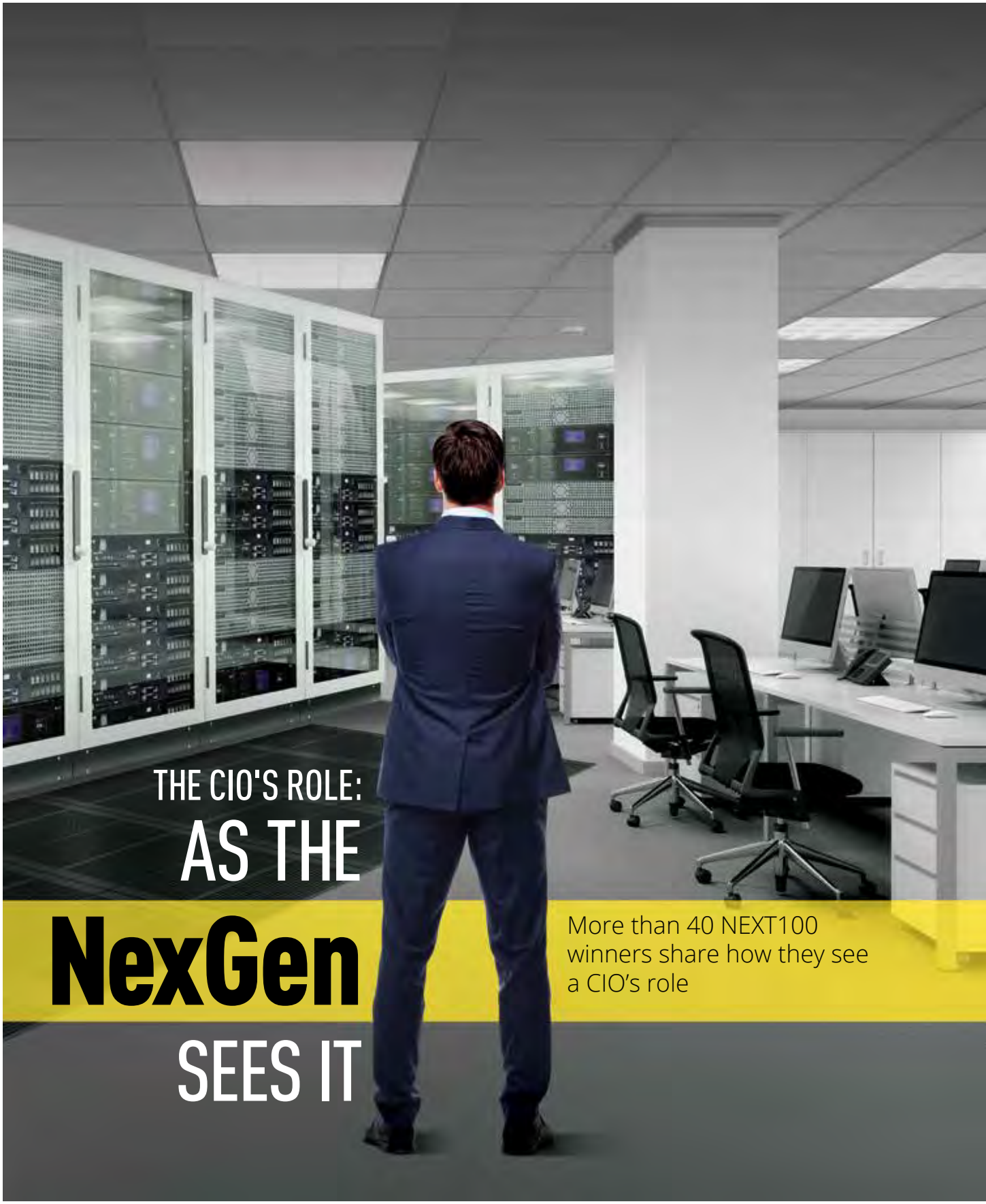
I have performed in a few events, especially in community get-togethers and college fests. I attended shows like Arijit Singh Live in Concert (India Tour), Aagomoni (an evening of music and festivity) 2018 by Mamata Shankar and troupe, Gulzar Ji with Bhupinder and Mitali Singh, Usha Uthup, etc.■

As told to Dipanjan Mitra, Team ITNEXT

Subhanil Banerjee

Snapshot

Subhanil Banerjee is Senior Manager – IT Infrastructure & Security at ABP. He is NEXT100 Winner 2017. He has worked in various managerial positions in companies like Orange Business Services, Emami and National Stock Exchange. He has done his BTech in IT.



THE CIO'S ROLE: AS THE NexGen SEES IT

More than 40 NEXT100 winners share how they see a CIO's role

More than 40 NEXT100 winners think of supporting business or aligning with business goals — already defined by someone else — is the role of CIO

By ITNEXT

The changing role of the CIO is—and has been—by far the most common discussed topic among CIOs.

But how do the future CIOs—the next-in-line—see the CIO role? We decided to find out—because these are the people who would get into the 'changed' role of CIO.

To figure that out, we decided to ask the best-in-class—the NEXT100 winners over the years. In the nine years since the NEXT100 started, there are 900 winners. About 650 of them are in the year-wise WhatsApp groups that we have.

We asked them a simple question on WhatsApp: How do you define the role of CIO today?

Forty-three of them responded with their responses. They are presented in the pages that follow.

But before you actually take a look at them and figure out what to expect from this NexGen IT leaders, here is a context and some insights from the exercise.

First of all—the question. We asked them to 'define' the role and not 'how they perceive the role to be'. The latter is their understanding of what their bosses do. The former is what their bosses or they themselves should do.

We also asked how they see the role 'today'. That was a deliberately vague reference to changing roles. We refrained from explicitly asking 'changing' because we did not want to influence them—that the role is changing. Secondly, we did not want them to talk about a very distant future. Basically, we filtered out kite flying.

So, what should it be?

So, how do these next-in-line leaders define a CIO's role?

While you will read that in detail, here is some good news and some bad news, looking at the answers.

The good news is that: We do not see any difference between their thinking and the thinking of CIOs.

The bad news is: We do not see any difference between their thinking and the thinking of CIOs.

That is not a typo. The good news and bad news are the same. Here is the explanation.

What the sentence means is this. Most next-

in-line leaders already think the role to be what the CIOs tell it is—from their experience. There is an increased sensitization that understanding business, business alignment, creating business value is most important. There is still a perception that the IT managers talk too much about technology and do not appreciate business issues. That is most definitely shattered—what with 'business' being the most repeated word across all answers.

In short, there is little gap between what the CIOs think and what the NexGen thinks.

That is the bad news. One expects the NexGen, much younger than CIOs—thanks to India's demographics—to think differently. Business and tech landscape is changing. Technology is changing business models. It is showing age old companies what to embrace, what to abandon. Yet, most of these future CIOs think of supporting business or aligning with business goals (already defined by someone else) is the role of CIO.

The thinking is not changing as fast as the rules are changing. While the next line IT managers could have learned to speak the language of business, they still do not think like disruptors—even if there is a generous use of the word 'disruption' in some answers.

That is a little disappointing.

Having said that, there are people who talk about 'changing the world'. That implicitly implies leading change. But such examples are few.

The buzzwords

Business itself, as you can see in the word cloud, is the top buzzword. It appears in various contexts.

'CIO must possess strong business acumen.'

'A CIO runs business with innovative technology.'

'A CIO is involved in alignment of new technology to improve and ease business delivery.'

'Creates business value through technology.'

Leadership is another such recurring attribute.

Alignment, digital, technology are the other frequently recurring themes.

Yes, there is vision, value and strategy too.

But the underlying story is this: Today's next line is ready to grab the CIO role. They exactly understand what is expected from them. For 90% of the businesses, that is what they want. There is good news for them: The pool is big.

Those who want to bring in disruptive change may have to look for disruptive ideas themselves or select the bright and give them a blank canvas to prepare themselves before they can entrust the top role to them. ■

Winners' Speak

A CIO is a business enabler, understands & implements organization IT strategy to realize benefits, sustainability, and relevance and develops high performing teams, shares vision & objectives

– Ajit Kanitkar, Manager – Project Services, Tieto
(NEXT100 Winner 2016)

CIO must possess strong business acumen and ensure employees have right technology and tools to enable company's core business

– Amit Ambre, Senior Project Manager, Tieto
(NEXT100 Winner 2018)

A CIO is an innovator in an ever-changing business world

– Amit Phadke, VP – Global IT Infrastructure and Security, Accelya Group
(NEXT100 Winner 2010)

A CIO is a visionary storyteller who is committed to changing the world with technology and knows very well that only paranoid survive

– Amitesh Tyagi, Director, Nielsen
(NEXT100 Winner 2017)

A CIO is an innovator, strategist & thinker who thinks beyond technology, competes effectively and responds to industry demands

– Anand Gaikwad, Senior Manager – IT/Global Program Manager, Volkswagen IT Services India
(NEXT100 Winner 2017)

A CIO needs to focus on key areas like technology and must possess business acumen and have the right attitude for automation

– Aniket Shah, Associate Vice President, Kotak Mahindra Bank
(NEXT100 Winner 2018)

CIO has to observe the digital changes in the organization. Real-time operational performance, integrated performance management, scenario-based risk assessments are current KPIs of CIO in industry

– Anil Kumar, DGM – IT, Maharashtra Seamless
(NEXT100 Winner 2018)

A CIO is a visionary leader creating value for an organization through technology disruptions leading to simplification, integration and digitization of business processes

– Ankit Aggarwal, Head – IT (Udaipur), PI Industries
(NEXT100 Winner 2018)

A CIO is a senior level officer who acts as a bridge between business and technology and aligns technology to business efficiencies and requirements

– Anuj Joshi, Associate Vice President, Evalueserve
(NEXT100 Winner 2012)

A CIO is someone who blends IT and business agility. He/she is a business partner who defines, articulates and champions organization's strategic and operational plans, identifies where business needs support to grow and stimulates growth

– Ashok Nayak, Chief Information Officer, Ipca Laboratories
(NEXT100 Winner 2016)

A CIO is involved in the alignment of new technology to improve and ease the business delivery with speed and accuracy. He/she is equally responsible for business improvement

– Ashwini Kumar, Head – IT Applications, Shalimar Paints
(NEXT100 Winner 2018)

The power of CIO and his/her business process clarity is unmatched

– Atul Vij, Group President, Auto Components Sector
(NEXT100 Winner 2012)

CIO plays the role of a bridge, working with both sides: Business and IT. He/she is an enabler in business growth

– Bhavita Saxena, On-demand-CIO, Consultant – IT Strategy, Program/Project Manager, Consulting Ark
(NEXT100 Winner 2010)

A CIO is a leader with strong business acumen, technology adoption and people enabler who takes the organization to next level

– Bhushan Hukeri, Associate Vice President – Infrastructure Operations, Accenture Services
(NEXT100 Winner 2018)

CIO position is a much more strategic position, business as well as technology

– Claude Vaigas, Solution Architect, Consultant/Self-employed
(NEXT100 Winner 2010)

A CIO runs business with innovative technology and processes to achieve organizational objectives

– Gyan Prakash Srivastava, Senior Manager – IT, Hofincons Infotech & Industrial Services
(NEXT100 Winner 2016)

The role of CIO is framing organization's digital strategy, and leading digital innovation, such as strategic technology and planning

– Krishna Mohan, Deputy General Manager – IT, TV Sundram Iyengar & Sons
(NEXT100 Winner 2018)

CIO is someone who leads the company with all new technologies which is cost-effective and helps the business grow without compromising IT security

– Manish Surve, IT Infrastructure Head, Raychem RPG
(NEXT100 Winner 2016)

A CIO adopts and transforms technology without compromising business ethics, which boosts organizational efficiency within budget with maximum output

– Md. Shafi Shaikh, Senior Manager – Information System Administration, Agro Tech Foods
(NEXT100 Winner 2015)

A CIO needs to appear & evolve in the Board Meeting as an unimaginable identity to drive the entire conversation and flood with innovative ideas & emerging technology spearheading all the odds to deliver unexpected results within the desired timeframe

– Nikhil Kumar Nigam, Associate Director - Technologies, Amity University
(NEXT100 Winner 2015)

CIO ensures innovation and builds a technology enabled and data driven organization

– P Jayakrishnan, Associate Vice President, Muthoot Pappachan Technologies
(NEXT100 Winner 2016)

A CIO understands and prioritizes the business requirements, and drives business value through the use of best-fit and scalable technology

– Parveen Sharma, National Director – IT, Shardul Amarchand Mangaldas & Co
(NEXT100 Winner 2018)

The role of the CIO is to help set and lead the technology strategy for an organization, in concert with the other C-level executives. CIO has to provide an executive-level interface between the technology department and the rest of the business

– Pragnesh Patel, General Manager, Reliance Power
(NEXT100 Winner 2013)

A CIO is someone who has the right attitude to be representing IT into business and in the board rooms

– Ramkumari Iyer, CIO, Reliscale
(NEXT100 Winner 2015)

A CIO is a technology leader who understands the business and drives digital transformation using modern technologies to achieve business objectives

– Rajendra Bhandare, Vice President – IT, IDFC Securities
(NEXT100 Winner 2018)

A CIO role is an executive leadership role, enabling IT for business, defining IT strategy and roadmap and participating in boardroom decisions

– Rakesh Pandey, IT Service Delivery Lead, Zones
(NEXT100 Winner 2018)

A CIO aligns IT service, provides innovative solutions to add value to business in meeting end client requirements

– Ramesh Sharma, Senior Director, Capgemini Technologies Service
(NEXT100 Winner 2018)

A CIO is someone who creates business value through technology, laser focus on operations and security, and is a visionary with strategic view

– Ravindra Prasad Elecherla, Director, ADP
(NEXT100 Winner 2010)

CIO is a professional who is technology evangelist and also has business acumen for creating symphony of business and technology

– Sandeep Jamdagni, AGM – IT, Ashiana Housing
(NEXT100 Winner 2016)

A CIO is someone who creates business value. He/she ensures that tech systems and procedures lead to outcomes in line with business goals. He/she aims towards building and maintaining an effective and motivated team

– Sanjay Chhokra, Head – IT, Nirmal Vision for Vision Society
(NEXT100 Winner 2013)

The CIO role is an important line function role directly linked to profit maximization through business and operations internal process improvement

- Saritha Kaza, Deputy General Manager, Toshiba Transmission & Distribution Systems (India)
(NEXT100 Winner 2010)

CIO is a business leader who has vision to build data and right technology, which in turn drives decision making

– Shelton Vetharaj, Global DevOps Manager, Coats
(NEXT100 Winner 2010)

A CIO is the one who takes his/her organization into the next orbit, selects the best breed of technology and optimum adoption to transform the business towards digital

– Shreyas Dukle, CIO, Mahindra Partner Companies & Group CIO Office, M&M
(NEXT100 Winner 2012)

A CIO is a leader who understands end-customer expectations and aligns it with business goals by providing the right technology tools to internal teams

– Shweta Srivastava, Chief Technology Officer, Paul Merchants
(NEXT100 Winner 2018)

A CIO is a digital crusader who enables the business with state-of-the-art technology, clear value articulation of IT and continuous innovation

– Srikanth Mattipalli, Enterprise Solutions Architect, Consultant
(NEXT100 Winner 2013)

A CIO needs to focus mainly on digital to avoid being the digit 0 of the Binary Number Theory!

– Srinidhi Narayan, Head Program Management Office – Group IT, Piramal Enterprises
(NEXT100 Winner 2018)

A CIO is a strategist who can co-create current and future vision of the organization and is also able to execute it

– Sushma Chopra, Assistant Vice President – IT, Sony Pictures Networks India
(NEXT100 Winner 2013)

CIO should be the first learner of emerging technologies and must know about business transformation using emerging technologies

– Venkata Ramana Ratnakaram, Group Head – Operations (Technology), Manappuram Finance
(NEXT100 Winner 2015)

CIO is business process functional expert, good team leader & mentor, passionate innovative technologist, focuses on progressive cost optimizations and is an IT solutions architect

– Venugopalam Medicherla, Chief Information Officer, Mro-Tek Reality
(NEXT100 Winner 2016)

A CIO is someone who ensures all IT services are running within budget and are acting as business catalyst

– Vinod Ahuja, Head – IT Infrastructure Management Services, Atos India
(NEXT100 Winner 2016)

A CIO is someone who looks for corporate IT strategy and business and works closely with other CXOs to transform internal and customer facing processes using technology

– Vishal Jain, Head – IT & Infrastructure, Espire Infolabs
(NEXT100 Winner 2012)

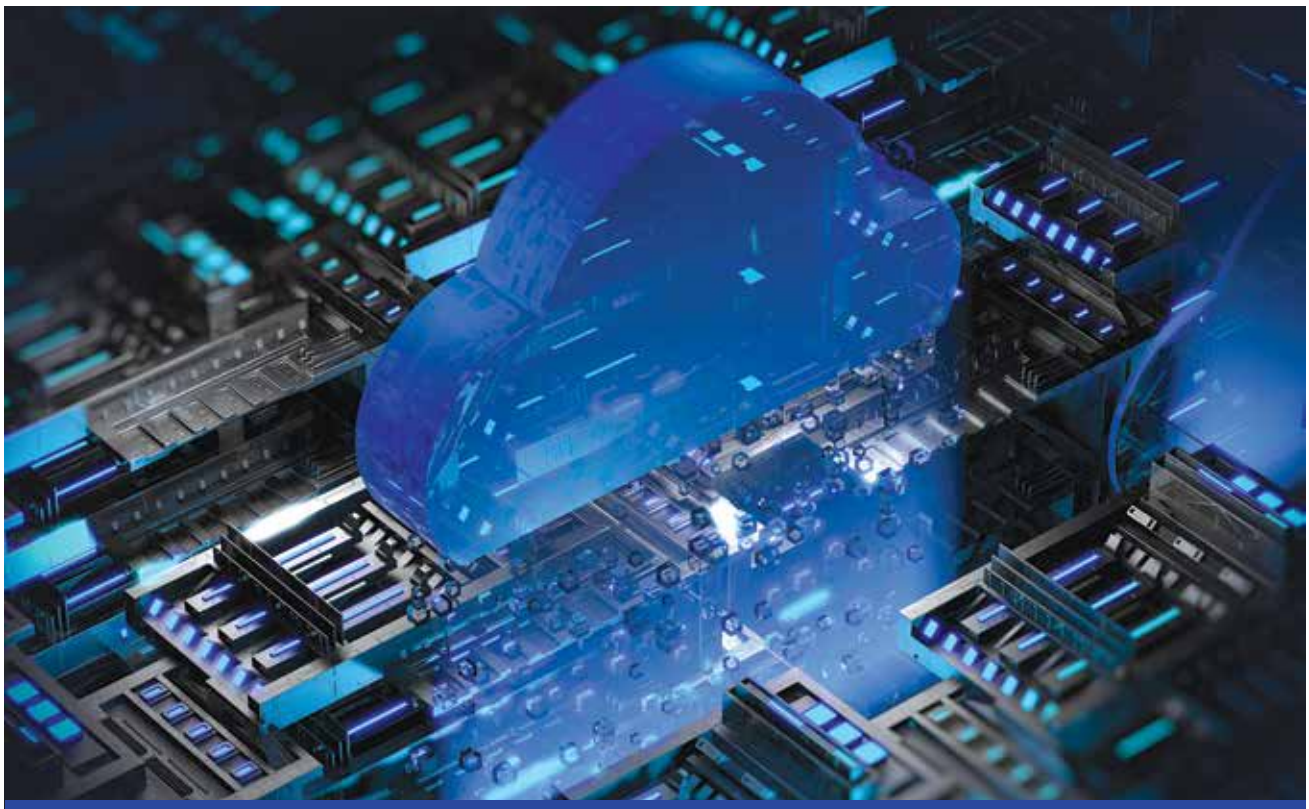
CIO is centrifugal force today, enabling organizations to achieve targets, providing future ready technologies and provisioning smooth customer interactions

– Yatin Bhatia, Assistant Vice President – Technology, Aptech
(NEXT100 Winner 2012)

A CIO needs to have product quality focus with profitability to the organization while enriching customer experience

– Yogesh Dadke, Asia IT Leader, Adient Technologies
(NEXT100 Winner 2018)

But the underlying story is this: Today's next line is ready to grab the CIO role. They exactly understand what is expected from them. For 90% of the businesses, that is what they want. There is good news for them: The pool is big. Those who want to bring in disruptive change may have to look for disruptive ideas themselves or select the bright and give them a blank canvas to prepare themselves before they can entrust the top role to them



Why Should Enterprises Not Be Wary of Hybrid Cloud Environments?

It is worth piloting the latest Hybrid Cloud Technologies offered consistently on both on-premises and public cloud as they offer vastly superior support as a fillip to your hybrid cloud journey

By B.S. Nagarajan

Global ramp and reach ambitions of businesses of all sizes are becoming more achievable just as consumer demand for them to be more agile and accessible are becoming more strident. Digital transformation strategy with hybrid cloud computing at its core is being embraced by diverse businesses as an effective solution to enable dramatic business growth. With the recent advances announced by us in collaboration with leading public cloud providers, hybrid cloud comes back to the center as the pivotal element of a winning digital transformation solution.

However, one element that hampers most decisions in moving to hybrid cloud is the dreaded application migration from legacy, on-premises to hybrid cloud environments because they are

rendered complex due to typically extensive redesign and code refactoring needs before any migration can happen. Businesses have to either commit to redesigning the applications in-house or to outsource it to SIs (System Integrators). It can take many weeks or months of development and testing just to migrate the applications. There is often another caveat. Once the migration is completed, it could take an equally complex process if businesses were to decide to retract the migration and go back to their previous environment.

A customer I know had been lamenting that it had taken them 8 months to retract their migration. They had already taken over a year to execute the migration processes that included extensive redesign. While the time lost in this process is certainly very high, we are not even attempting to quantify the disruption and distraction caused within the organization during the whole episode. Another customer spent over 2 years exploring leading Public Cloud Service providers but, was still unsure about his next steps at the end of it. When we introduced the recent trailblazing advances in collaboration with leading public clouds, it took customers a long time to be convinced that they could indeed create a limited hybrid cloud environment within days instead of months.

Several customers have checkered experiences like this and are consumed with protracted and inconclusive pilots. It really gets down to whether they can commit to a long and complex application migration that will occupy the bandwidth of their development teams in a big way. Many customers are wary of the possibilities and opportunities of hybrid cloud even when they are introduced to what is now possible using the latest DC technology advances: Zero-minimum migration effort, Full portability of applications to Cloud, Live (yes, you read it right, LIVE), bi-directional movement of workloads and consistent technology stack on both on-premises and cloud.

While we can empathize with them on their pilot fatigue, it is pragmatic to commit to a focused and thorough study with the most advanced hybrid cloud technology available and watch their development teams migrate their applications live. For instance, a BFSI customer has recently migrated 400 applications in 2 days, another customer has migrated 650 applications in 5 days while another globally reputed educational institution in the US has migrated 3000 applications in 45 days against an earlier estimate of 30 months using what was available earlier. These claims may seem unbelievable and almost impossible, but they are worth validating and realizing.

Top Reasons for Piloting the Latest Hybrid Cloud Technologies

Whatever your earlier experiences, it is worth piloting the latest hybrid cloud technologies offered consistently on both on-premises and public cloud as they offer vastly superior support as a fillip to your hybrid cloud journey.

Effortless Migration

- Migration is effortless and almost instantaneous due to consistent technological environment on both on-premises and cloud environments
- Migration can be done live without any downtime

- Applications can be shifted back and forth as needed
- No need to redesign or refactor existing applications

Low Risk

- A starter configuration of a Single Host is all that is needed to commence a pilot
- Suitable for development-test workloads due to limited availability commitment
- Needed investment is negligible in an enterprise IT budget

Efficient and Swift On-boarding

- Hybrid cloud pilot environment is extremely quick to provision
- The alternative of refreshing an existing or creating a new on-premises environment takes many months just to set up
- Most of the pilot time is spent in analyzing the core application experiences instead of being consumed in preparation and set-up

A Step in the Right Direction

A swift pilot to test the latest advances in hybrid cloud technologies and their consistency with on-premises environments is too valuable to miss. Despite being wary based on earlier experiences with long and complex pilots, it is an incredible opportunity to validate the cost, process, effort, ease and flexibility that the new possibilities offer.

It's no surprise that NPCI (National Payments Corporation of India), the largest digital payment provider in the country, has migrated its business critical systems to cloud. There is absolutely no stopping customers now and no source of concern as long as they understand the possibilities that hybrid cloud offers to their specific business scenarios. They can move towards hybrid cloud with certainty and conviction. It will be a step in the right direction. ■

The author is Senior Director and Chief Technologist, VMware India

Artificial Intelligence: Changing Healthcare Landscape

Any new age technology adoption will face 'Iron Triangle' of healthcare test to prove its worth

By Sanjay Pathak

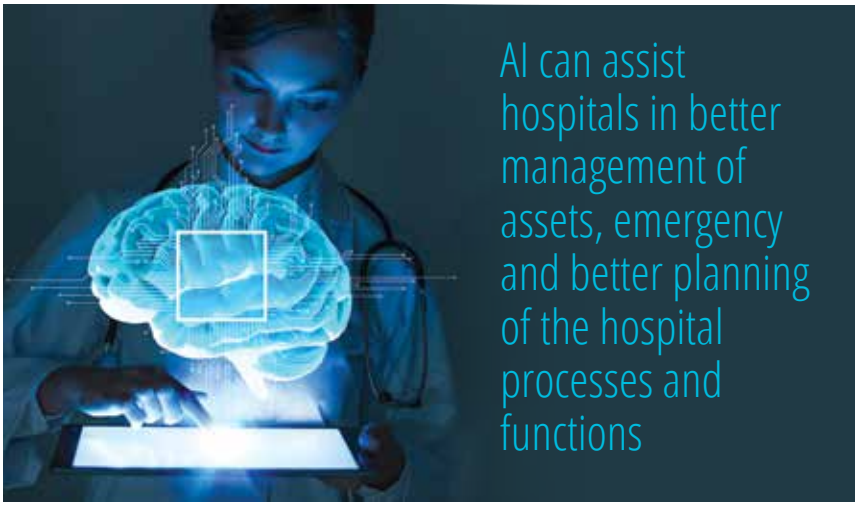
Looking at the upcoming trends globally and across industry 'Artificial Intelligence/ Machine Learning (AI/ML)' tops the charts. Generally, first thing which comes to mind is machine/cyborg taking over human elements and this has been depicted to various degrees in many sci-fi movies. While, the reality is far away from that, it will be unjust to ignore how healthcare is evolving and adopting AI in real life to reduce cost and improve patient outcomes.

In current context, AI means simulation of human elements by machines/computers, where they acquire information (learning), process it to reach reasonable conclusions (action) and adapt themselves to situations (course corrections). AI leverages various technologies like Machine/Deep learning, Vision, NLP, Robots or autonomous machines, etc.

As per Gartner, most organizations are in early stage of AI adoption. Only around 6% have it in use and more than 60% organizations are still trying to understand it. It will take a while before real benefits of AI can be leveraged. Below are areas where AI has

already made its way or can bring in difference in future:

1. Leveraging vision, deep learning on sensor-based vital data, physicians will be better equipped to diagnose ailments. Medical imaging can be taken to new levels where AI on top can accurately diagnose and in some cases even predict diseases. Blood smears will use vision to count cells and anomalies. ECG & cardio data can pass through Alto predict outcomes and assist physicians in accurate diagnosis.
2. Hospital re-admission has been a grave concern and millions wasted due to lack of post operation care. AI can help predict situation like this and can assist providers take extra precautions.
3. Based on the patient case and required procedures, AI can help in planning surgery, help doctors in accurate measurements, and assist during surgery by tracking vital and other data. AI can help surgeons understand surgery outcomesbetter based on correlations from similar cases.
4. Using NLP and vision, AI can assist doctors with diagnosis, running pharmacy correlations with other drugs, allergy, food etc. AI can help physicians with transcripts and voice assisted case management. All these integrated with EHR system will bring in the best of the best values.
5. Virtual health assistants are tools like chatbots or a conversational service using smart speakers helping customer answer health related quires, symptoms checker or assist them with appointments.
6. AI can assist hospitals in better management of assets, emergency management and better planning of the hospital processes and functions.
7. In the field of telemedicine, AI can bring wonders by enabling accurate remote health monitoring, predictive diagnosis leading to cheaper & effective remote/rural health management.



If we flip to other side of healthcare, that is, 'insurance', AI can bring many value-added services together with care side to bring down the overall healthcare spending globally.

1. Outcome, risk and cost comparison for similar cases in different hospitals/cities will help insurance companies compare cost and better optimize the plans offered and their premiums.
2. Predictive element of care can assist providersin better reach out to patients and proactive care management, which can save significant amounts for both sides.
3. Predictive AI for care, claims and other information can also help providers come up with health plans, which are cheaper and more effective.
4. AI systems can sift through clinical and claims data to highlight errors in diagnosis, payments, frauds and workflow issues, thus providing a true value based care system.

The real test for AI system will depend on solutions' ability to integrate with the hospital or doctors' workflow. AI systems should not be perceived as extra process, as that will reduce the value such systems can potentially bring.

Adoption of AI in healthcare, both clinical and insurance will be slow and will face some challenges like:

1. Ethical concerns due to reduction in Hu element- who takes the liability for a negative event?
2. Regulation & compliance will play a big role in adaption of AI as they will govern the process and procedures that are followed.
3. Initial adoption both by physicians and patients will see hiccups mostly related to trust factors, till the time both parties build confidence in such systems.
4. Lack of requisite skillsets for technology adoption, followed by trainings of end users.

AI or any new-age technology adoption will face 'Iron Triangle' of healthcare (access, quality, and cost) test to prove its worth. For an industry which has always lacked skilled manpower to manage everyone's health, AI can do wonders. ■

The author is Head - Healthcare & Insurance Solutions at 3i Infotech

Securing Enterprises While Using SaaS Applications

Using a Cloud Access Security Broker (CASB), IT will be able to monitor all activities and enforce security policies including securing data on personal devices, limiting external sharing, detecting and preventing cloud malware

By Vikas Yadav

SaaS applications are becoming a reality with cloud-first policy and the ease and convenience of deploying new applications. According to Gartner, more than 50% new software purchases are likely to be via SaaS and new models of purchase. But this is giving rise to increasing security challenges as businesses take the initiative directly without consulting IT.

So can IT proactively engage with the organization to participate, prevent and safeguard from new risks? As I see it, IT led by the CISO can manage the challenge of shadow IT with a three-pronged approach: educate users; establish pro-

cesses for procurement and deploy technology to secure the organization.

Educating Line of Business

Often businesses are not aware of the security risks of buying application directly and IT must take the initiative to educate businesses about the associated risks. While doing this, it is important to understand the buyer/business perspective.

For instance, buying experience in SaaS is completely different from traditional software wherein SaaS allows free trails and pricing is readily available. Therefore, business managers feel IT managers can be eliminated from the buying process. This also means that while the business head may be the buying decision maker, the person who evaluates SaaS maybe someone else.

Therefore, IT initiative to reach out to business users must be enterprise-wide—encompassing all levels of employees—explaining the nuances of security, performance challenges arising out of compatibility issues and integration challenges.

Establishing Process and Control

IT must have a collaborative approach to win over line of business managers by providing the right information to empower businesses to make the right decisions.

There must be established processes to involve IT in buying decisions from evaluation stage to assess security risks including where the service is hosted, who the infrastructure service provider is; what kind of access will be required to enterprise resources; and what kind of IT support is needed.

Often businesses end up buying overlapping applications and services creating a SaaS sprawl, which increases security risks. However, by involving IT early via established processes, this can be eliminated. Sometimes an existing SaaS application may require minor modification or extensive customization to meet the needs of business in which case IT will need to take a call collaboratively with business after evaluating internal capabilities.

Ideally, SaaS applications must have integrations with HR to ensure employees who leave the organizations do not have access to the SaaS application.

Technology Intervention

Once buying decisions have been collaboratively made, IT must ensure that SaaS is securely deployed in the organization. This means assessing the criticality of data stored in the cloud, who is accessing what kind of data and what kind of controls are put in place.

Using a Cloud Access Security Broker (CASB), IT will be able to monitor all activities and enforce security policies including securing data on personal devices, limiting external sharing, detecting and preventing cloud malware. A robust CASB solution can mitigate both internal and external threats by restricting data access and track and monitor behavior of users.

Increasingly, best-in-class enterprises are relying on zero-trust architecture to secure SaaS applications. This means every request by any user or machine is properly authenticated, authorized and encrypted. It calls for strong configuration of identity and access management; enforcing permission, authorization and privilege access rigorously to deliver granular access to resources while ensuring visibility and transparency.

As corporate networks extend beyond the firewall, IT is increasingly challenged to evolve and claim its status as the custodian of organizational security. To do this, IT must be allowed to lead the CISO office to engage proactively with business and become a partner in achieving business objectives while meeting security goals of the organization. ■

Often businesses are not aware of the security risks of buying application directly and IT must take the initiative to educate businesses about the associated risks

The author is CISO at Max Life Insurance Co

Why CIOs Should Pay Attention To 5G Revolution

The transition to 5G can be touted as a game changer for organizations. But to take full advantage of its many capabilities, CIOs must have a digital strategy in place

By Sohini Bagchi

5G, or the next-generation of wireless systems is bringing about a sweeping change not only in the telecom industry, but also in the enterprise and consumer space. Considered a 'hype' until recently, today, it is fast becoming a reality, as many countries across the world – including India – are already investing in 5G (or are planning huge investments in the near future) in order to gain from its high-speed network and reliability.

5G is poised to be at least 10 times faster than 4G, and several times more responsive than its predecessor. Further, 5G is expected to connect 100 times more devices than 4G did, giving rise to a deluge of IoT-enabled gadgets and devices. The evolution of 5G should certainly be of interest to C-level executives such as Chief Information Officers (CIOs). However, they will need to upgrade their skill-sets in order to ready themselves for an ultra-fast future.

A recent research by tech analyst firm 451 Research and Vertiv, that polled over 100 global telecom decision makers with visibility into 5G strategies and plans, shows that enterprises are overwhelmingly optimistic about the 5G business outlook and are moving forward aggressively with deployment plans.

The reason for optimism among businesses is that they could benefit from more real-time online interactions with customers, have seamless video conferences with staff, and have a more connected and efficient network for real-time interactions and run complex applications effortlessly. In other words, 5G is poised to solve some of the most critical business problems and hugely improve bottomline.

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

According to the survey, most of those initial services will focus on supporting existing data services. About one-third of respondents expect to support existing enterprise services with 18% saying they expect to deliver new enterprise services.

The Telco Readiness

As networks continue to evolve and

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

However, illustrating the scale of the challenge, nearly 68% telcos in the survey said, they do not expect to achieve total 5G coverage until 2028 or later. 28% expect to have total coverage by 2027 while only 4% expect to have total coverage by 2025.

"5G presents a huge opportunity for India, further revolutionizing the app and content ecosystem in the country. The world over, telcos have recognized this potential, while also understanding the network transformation required to support these services," says Girish Oberoi, General Manager of Telecom Strategic Account Management for Vertiv in India.

To support 5G services, telcos are ramping up the deployment of Multi-access Edge Computing (MEC) sites, which bring the capabilities of the cloud directly to the radio access network. 37% of respondents said they are already deploying MEC infrastructure ahead of 5G deployments while an additional 47% intend to deploy MECs.

As these new computing locations supporting 5G come online, the ability to remotely monitor and manage increasingly dense networks becomes more critical to maintaining profitability. In the area of remote management, Data Center Infrastructure Management (DCIM) was identified as the most important enabler, followed by energy management. Remote management will be critical, as the report suggests the network densification required for 5G could require operators to double the number of radio access locations around the globe in the next 10-15 years.

In fact, telcos are also increasing network energy consumption. The study shows AC to DC conversions will be an area of emphasis. Besides, new cooling techniques will see the biggest jump in adoption over the next five years. Currently being used by 43% of telcos worldwide, this number is expected to increase to 73% in five years.

Upgrades from VRLA to lithium-ion batteries also show significant growth. Currently, 66% of telcos are upgrading their batteries. Five years from now, that number is projected to jump to 81%.

Despite the readiness, a Gartner report released in 2018 said there is still a lack of readiness among telcos and communications service providers (CSPs).

"While 66% of organizations have plans to deploy 5G by 2020, the CSPs' 5G networks are not available or capable enough for the needs of organizations," said Sylvain Fabre, senior research director at Gartner.

To fully exploit 5G, a new network topology is required, including new network elements, such as edge computing, core network slicing and radio network densification. "In the short to medium-term, organizations wanting to leverage 5G for use cases, such as IoT communications, video, control and automation, fixed wireless access and high-performance edge analytics cannot fully rely on 5G public infrastructure for delivery," added Fabre.

The CIO Challenge

While 5G network bandwidth and speed will undoubtedly facilitate a surge in high-bandwidth and real-time communications in organizations, it's going to have an absolute impact on IT strategic plans. This could be challenging unless the CIOs have a strong digital strategy in place.

Firstly, to unlock the level of intelligence and connectivity 5G promises, it is critical that wireless connectivity should be incorporated into the CIO's business plan. This means, in terms of employees' devices – whether bring-your-own-device (BYOD) or corporate devices they need to decide fast as to whether to upgrade to 5G and, if so, to identify the main use cases. A Gartner report notes that IoT communications remains the most popular target use case for 5G, with 59% of the organizations surveyed expecting 5G-capable networks to be widely used for this purpose. The next most popular use case is video, which was chosen by 53% of the respondents.

Secondly, CIOs need to address how 5G is going to affect the overall communications infrastructure. Until now, CIOs look at wireless infrastructure as a way of managing infrastructure for their Wi-Fi network and cellular has been an opex cost. 5G is different because the base stations need to be much more densely deployed and the form factors have shrunk dramatically. For example, in the US, several stadiums and train stations are integrating wireless LAN and cellular to offer a better user experience – a food for thought for CIOs. They must also plan for the different service layers needed to support the many new sensors for 5G applications.

Thirdly, CIOs should review/audit their present network infrastructures to understand what upgrades or replacements to network hardware, software, and services may be required to get ready for 5G and chalk out a budget plan as network upgrades are expensive.

Fourthly, CIOs and other IT leaders should be preparing for the 5G data avalanche now. Findings from Ericsson show there could be 3.5 billion Internet of Things units by 2023 — equaling five times the number of connected devices used now. Additionally, the company forecasts that 5G networks will spur the growth of Internet-connected devices. The CIO should filter and accept only kind of data and exclude the rest from network access. This requires a rigorous data planning. CIOs must ensure newer enterprise systems are being designed with a natural migration path to software-based systems, significantly reducing footprint, power, and cooling requirements while operating more like data center software.

Fifthly, transitioning to 5G will come with its own security risks. Experts

point out that 5G and the various new applications that will come with it will widen the arena for cyber criminals. For example, a team of researchers discovered issues with the 5G security protocol, known as Authentication and Key Agreement (AKA) – a standard associated with a communications protocol organization called the 3rd Generation Partnership Project (3GPP). The ETH researchers from the group headed by David Basin, Professor of Information Security, showed that the standard is insufficient to achieve all the critical security aims of the 5G AKA protocol. Hence, a poor implementation of the current standard can result in very serious security implications, unless CIO/CISOs work out stringent security measures while adopting 5G technology.

Finally, CIOs should embrace new technologies and business processes. With 5G, of mission-critical applications will move to the cloud. Needless to say, one of the constraining factors for cloud that exists today is bandwidth. But the bandwidth and data transfer capabilities of 5G will virtually remove this challenge and reshape IT strategies in the areas of application deployment, governance, and security. This will also prompt a need for IT to work closely with cloud vendors that can be entrusted as able stewards of sensitive corporate data and processing. CIOs should also upgrade their skills to dabble with technologies, such as Augmented Reality (AR), Virtual Reality (VR), IoT and Big Data, to name a few.

5G will undoubtedly force a wave of innovation around mobile technology, analytics, datacenters, cloud and IoT implementation. While the deployments are likely to be ambiguous at least in the initial years, as most 5G technologies are not yet proven at scale and nor is the cost of investment completely justified, 5G can be touted as a game changer for organizations. And CIOs need to get their heads around 5G, because it is coming their way. ■

Securing SWIFT Environment Within Banks

In order to strengthen the security, Indian regulator RBI also issued many circulars in this regard and even imposed penalties on 36 banks in March 2019 for non-compliance on SWIFT Operations

By Prakash Kumar Ranjan

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides a network that enables banks to send and receive information about financial transactions in a secure, standardized and reliable environment. SWIFT is commonly used by most of the banks in India for cross border inter-bank payments system. Now even SWIFT India is providing services for domestic payment system.

A series of cyberattacks using the SWIFT banking network has been reported in last 4-5 years. The first public report of these attacks came from Bangladesh Central Bank. We have also seen the attack at State Bank of Mauritius, COSMOS Bank and City Union Bank.

In order to strengthen the security, Indian regulator RBI also issued many circulars in this regard and even imposed penalties on 36 banks in March 2019 for non-compliance on SWIFT Operations.

SWIFT has also come up with Customer Security Program (CSP) wherein they have released a security baseline for the entire community and must be implemented by all users on their local SWIFT infrastructure.

The controls in the CSP revolve around three objectives:

1. Secure your environment
2. Know and limit access
3. Detect and respond

What banks should do to strengthen the SWIFT infrastructure and operations:

1. Isolate the general IT environment from SWIFT infrastructure.
2. Disable USB, email, Internet from SWIFT workstations.
3. Restrict the gateway timings as per their business requirement and integrate the same with SIEM for proper monitoring and reporting any anomaly detection.
4. Patch the servers and endpoints regularly.
5. Monitor the user logon activity through SIEM and reporting any anomaly detection.

A series of cyberattacks using the SWIFT banking network has been reported in last 4-5 years. The first public report of these attacks came from Bangladesh Central Bank. We have also seen the attack at State Bank of Mauritius, COSMOS Bank and City Union Bank

6. Regularly review the existing RMA (Relationship Management Application) and remove the obsolete RMAs.
7. RBI has asked all banks to integrate the SWIFT with CBS for both financial and non-financial messages, however still many banks has not implemented STP (Straight Through Processing) for non-financial messages. So, bank should integrate SWIFT with SIEM and any direct message created in SWIFT should be reported immediately.
8. Regularly reconciling the NOSTRO account.
9. If any bank is using middleware applications between SWIFT and CBS then they should do online reconciliation using any recon tool to reconcile messages generated in middleware and SWIFT.
10. Ensure SoD (Segregation of Duties) in letter and spirit.
11. Monitor the activities of privileged users in SWIFT system using any PIM/PAM tool.
12. Vulnerability Assessment (VA) should be carried out periodically.
13. Implementing Multi-factor Authentication (MFA) in both CBS and SWIFT.
14. Logs of SWIFT infra should be sent to SIEM and SOC should monitor integrity check of both software and database.
15. Create, publish and test the Incident Response Procedure and conduct table top exercise frequently.
16. Lastly, awareness of security should be mandatorily imparted to all users as security is a shared responsibility. ■

The author is ICT Security Risk & Compliance Manager, CNH Industrial

CIOs In Financial Sector See Silver Lining In Hybrid Cloud Adoption

The sector still runs a significant percentage of traditional datacenters and is struggling to find the best IT talents

By Sohini Bagchi

Financial services firms today are facing mounting competitive pressure to streamline operations while delivering a differentiated experience to their customers, including leveraging new technologies such as blockchain. This FinTech revolution, combined with the growing burden of regulatory compliance, data privacy, and security issues are pushing CIOs to fundamentally transform the technological underpinnings of their institutions.

In view of that, a new report released by Nutanix, many financial organizations are still struggling with modernizing their outdated legacy IT architectures and processes, resulting in inefficient operations and potential vulnerability with

regards to data breaches. In fact, the report revealed financial services run more traditional datacenters than other industries, with 46% penetration. Despite their progressiveness on the hybrid cloud front, financial organizations have lower usage levels of private clouds than any other industry, at 29% penetration compared to the average of 33%.

The survey conducted by Vanson Bourne that polled over 2,300 IT decision makers worldwide including India, observes, like other industries, the financial services sector cites security and compliance as the top factor in deciding where to run its workloads. Nearly all respondents also indicated that performance, management, and TCO are critical factors in the decision. However, more than 25% cited these same factors as challenges with adopting public cloud. In other words, as is often the case with new IT solutions, the most important criteria are also the most difficult to achieve. This could account for part of the disparity between the high desire to adopt hybrid cloud, and today's relatively low hybrid cloud penetration levels of just 21% in the financial services sector.

"Legacy systems and processes are significant impediments to the agility that today's business demands. The BFSI segment in India has been a trailblazer in adoption of new tech such as HCI, Hybrid cloud, AI and ML," Sankarson Banerjee, CIO, RBL Bank says, adding that at RBL, Hybrid Cloud is at the forefront of our IT vision and strategy for driving agility in responding to business and customer needs across channels and products."

The positive outlook for hybrid cloud adoption globally and across industries is reflective of an IT landscape growing increasingly automated and flexible enough that enterprises have the choice to buy, build, or rent their IT infrastructure resources based on fast transforming application requirements.

However, challenges do exist. The report reveals that IT skills are a barrier to adopting hybrid cloud in the financial industry. While 88% of respondents said that they expect hybrid cloud to positively impact their businesses, hybrid cloud skills are scarce in today's IT organizations. These skills ranked second in scarcity only to those in artificial intelligence and machine learning (AI/ML). Financial services respondents generally reported slightly greater deficits in skillsets across all categories except for AI/ML.

The positive outlook for hybrid cloud adoption globally and across industries is reflective of an IT landscape growing increasingly automated and flexible

91% of financial services organizations surveyed said that hybrid cloud was the ideal IT model. This belief in hybrid cloud, and the fact that the sector has higher than industry average adoption of hybrid cloud, is likely driven by the recognized need for digital transformation. Yet conversely, the data shows a lower adoption of private clouds than the global average across industries. This might be explained by the fact that portions of the financial services space have been change-averse and also an indication of the overall complexity of modernizing existing legacy infrastructures.

"Increased competition combined with more stringent regulatory and compliance environments is forcing the entire industry to re-assess the capability and relevance of its current IT infrastructure," says Neville Vincent, Vice President A/NZ, ASEAN and India, Nutanix. Vincent however believes, the good news is that the industry is already seeing the customer and company benefits of hybrid cloud infrastructure. But he raises a word of caution to the CIOs. "The concern is that at just over 20%, there is still a long way to go to satisfy increasingly sophisticated and demanding customers and achieve the ultimate customer experience," he concludes. ■

CIOs Are Prime Victims In The Security Blame Game: Study

61% CIO/CISOs and security professionals have experienced a data breach at their current employer, according to McAfee

By Sohini Bagchi

Data breaches are becoming more serious as cyber criminals continue to target intellectual property, putting the reputation of company brand at risk and increasing financial liability. As a result of this, CIOs and CISOs are in a tight spot, constantly struggling to secure their organizations and protect them against breaches, says a new study, adding that they are often accountable for not being able to prevent data breaches.

According to a recent report by cyber security firm, McAfee, 61% CIO/CISOs and security professionals have experienced a data breach at their current employer, while 48% reported the same at their previous companies. Also, in the last three years, organizations facing serious data breaches that required full public disclosure have gone up from 68% to 73%, the report claims.

43% of the participants were greatly concerned about theft of personally identifiable information and intellectual property. On the other hand, 30% found theft of payment card details more distressing, even though the report claims that payment card is not a big target because of new payment technologies and improved fraud detection systems.

The concern over the personally identifiable information is higher in Europe due to the roll out of General Data Protection Regulation (GDPR) in May 2018, which mandates heavy

penalty on companies for failure to communicate data breaches to users. Theft of intellectual property is a bigger concern in the Asia-Pacific region, states the study.

Another interesting finding of the report is that cyber criminals do not have a singular technique when it comes to stealing data. In addition to database leak and interception of network traffic, they are also targeting corporate email, personal email, cloud applications as well as removable USB drives, stolen computers and printers.

CIO/CISO Struggling to Combat Data Breach

The McAfee report was based on a survey involving up to 5,000 professionals in enterprise organizations, over 5,000 workers in enterprise organizations and 700 IT and security professionals. The participants were based in the US, the UK, India, Australia, Canada, France, Germany and Singapore.

Over half of the participants blamed IT teams for not being able to prevent data breaches, while 81% are of the opinion that cyber security solutions continue to operate in isolation, with separate policies or management consoles for cloud access security broker and data loss prevention. This is causing delays in detection and reaction.

On the other hand, CIOs and CISOs interviewed in the study, feel part of the blame lies with C-suite, with 55% saying they feel that C-level executives should lose their job if data breach is serious as many of them often insist on having more lenient security policies for themselves.

Focus on Training and Culture

Many participants feel the cyber security attacks can be significantly reduced with education on corporate policies and appropriate online behavior. Real-time threat detection is also considered to be an effective way to identify threats. About 52% of all organizations have teams working on threat hunting, while 30% are planning to join the bandwagon soon.

CIOs and CISOs feel part of the blame lies with C-suite, with 55% saying C-level executives should lose their job...

"Organizations need to augment security measures by implementing a culture of security and emphasizing that all employees are part of an organization's security posture and not just the IT team. To stay ahead of threats, it is critical companies provide a holistic approach to improving the security process by not only utilizing an integrated security solution but also practicing good security hygiene," says Candace Worley, vice president and chief technical strategist, McAfee in an official statement.

What CIO/CISOs Should Do

Based on the study findings, we believe, the need of the hour for organizations is to have a cyber security strategy that includes implementing integrated security solutions.

CIO/CISOs should work in close collaboration with the C-level executives to formulate strategies to combat cyber security. The IT and security professionals need empowerment to influence budget decisions, project decisions, even IT decisions. This will give organizations a good visibility of information security risk and help them in managing those risks accordingly.

Finally, there should be a proper thrust on employee training and an overall culture of security throughout the organization to reduce future breaches, as the study too recommends. For that the CIO/CISOs' voice needs to be audible beyond the IT department, across the entire organization, in other words, the management board. ■

For CIOs, Open Source Is More An Innovation Tool Than Cost Center

Although open source will significantly reduce costs, the biggest impact of will be to sustain innovation, said CIOs in a global survey

Open source has evolved over the past two decades and has now permeated into the modern enterprise landscape. While the message is loud and clear that a majority of the CIOs and technology experts are already using open source, a new study report conducted by Illuminas and sponsored by Red Hat, wants to go one step ahead to find out in what ways are they innovating with this technology.

In it's recently released 'State of Enterprise Open Source' report, Red Hat gauges the landscape for adoption and usage, based on 950 interviews with IT leaders worldwide. As Jim

Whitehurst, CEO of Red Hat, stated in the report, "The question is no longer whether your enterprise should adopt open technologies; the question is when—and how."

Here are some takeaways for the CIOs from the study report.

Open Source is Strategically Important for CIOs

The CIOs who took the survey believe that Open source is strategically important to their organization's overall enterprise infrastructure software strategy. A whopping 69% said it was very or extremely important and only one percent said it was not important at all. The study noted that these CIOs have ramped up their use of open source and expect this to continue. Over two-third have increased their use of enterprise open source over the past 12 months and more than half—59%—expect to continue to do so over the next 12 months.

Open Source Paves Way for Digital Transformation

Enterprise open source today is replacing proprietary software for many different purposes from virtualization to message buses to application servers, unlike a few years ago. CIOs of the study noted that open source software isn't just about swapping out old infrastructure for modernized replacements. 42% say they're using it for digital transformation. The central idea can be cost reduction, but the pace at which open source is helping to define and shape new approaches to infrastructure from containerization to software-defined-storage and networking, the report noted the technology is helping CIOs create new opportunities, new services, and new classes of customer value like never before.

A More Secured Framework

Attributes such as security and the availability of support are reasons enterprises continue to switch to open source software. "Enterprise open source software can be well-supported and more secure and reliable for sure. But the same could be said of software from many proprietary vendors. One of the things that's unique about open source is the way it enables individuals and organizations to collaborate to achieve common goals," the study noted.

Enterprise open source today is replacing proprietary software for many different purposes from virtualization to message buses to application servers

An Engine for Innovation for CIOs

Open source software as a development approach is fundamentally different from that used for proprietary software. One of the upshots is that many of the new categories of software are influenced by open source technologies, the study noted. Artificial intelligence, software-defined infrastructure, and cloud-native platforms are a few examples. In other words, much of the innovation in the software world today is happening with open source. The study for instance also clearly shows that Containers that largely run on Linux, has helped drive DevOps in recent years. Over the next 12 months, 67% CIOs and IT leaders stated that they expect their container usage to increase.

Organizations that depend on software to support their businesses (which is to say most of them) want to be able to tap into that innovation.

Conclusion

While open source has always been of interest to CIOs and IT pros, the report clearly noted in 2019, they are reaping a lot more from this revolution. The study observes, enterprise open-source use is increasing. Over the past 12 months, 68% of respondents said that their organization's use of enterprise open-source software increased. Looking forward over the next 12 months, 59% of respondents said they plan to further increase their use of enterprise open-source software.

Today, organizations are buying into software as a change agent rather than just a cost center and into enterprise open source as a central element of the software universe rather than something a bit scary lurking at the periphery, the study concluded. ■

Cybercriminals Becoming More Methodical And Adaptive: Study

Cybercriminals are deviating towards a more focused approach against targets by using better obfuscation techniques and improved social engineering skills as organizations improve in areas such as time to detection and response to threats

Cybercriminals are deviating towards a more focused approach against targets by using better obfuscation techniques and improved social engineering skills as organizations improve in areas such as time to detection and response to threats, according to Trustwave's *2019 Global Security Report*.

Key Findings from the Report Include:

- **Asia Pacific and retail lead in data breaches** – The Asia-Pacific region led in the number of data compromises investigated, accounting for 35% of instances and overtaking North America at 30%, down from 43% in 2017. Europe, Middle East and Africa (EMEA) came in third at 27%, followed by Latin America & Caribbean (LAC) at 8%. The retail sector experienced the highest number of incidences at 18%. The finance sector came in second at 11% and hospitality third at 10%, each slightly dropping from 13% and 12%, respectively, from the previous year.

■ **Email threats becoming more focused** – Spam messages analyzed containing malware significantly diminished in 2018, to 6% from 26% in 2017. This drop can be attributed to a shift in tactics to shorter, more regional campaigns from Necurs, the largest malicious spamming botnet. For example, sextortion email campaigns designed to dupe victims into paying large ransoms by playing on fears that compromising videos exist on the recipient was nearly nonexistent in 2017 yet rose toward the end of 2018 to account for 10% of all spam analyzed.

■ **Malware becoming harder to detect** – Slightly down from the previous year, the largest single category of malware encountered was downloaders at 13%. Remote Access Trojans (RATs) at 10% and web shells at 8%, both of which give attackers extensive control over compromised computers, were the second and third most common types of malware discovered. Memory scrapers and dumpers used to steal payment card numbers from point-of-sale (POS) systems saw a sharp decline from 16% in 2017 to just 8% in 2018 as Europay, Mastercard and Visa (EMV) chip technologies become more prevalent. 67% of malware analyzed used obfuscation to help avoid detection, an astounding leap from 30% the previous year.

■ **Denial-of-service tops database vulnerability patching** – The number of vulnerabilities patched in five of the most common database products was 148, up from 119 in 2017. At 62%, denial-of-service (DoS) vulnerabilities used primarily for disruption accounted for the most vulnerabilities discovered across all major platforms in 2018. Far more serious information disclosure and privilege-escalation vulnerabilities used to gain unauthorized access and manipulate sensitive data accounted for 8.7% and 8.1% of patching incidents, respectively.

■ **Social engineering: Cybercrime's favored method of compromise** – Social engineering was the top method of compromise in 2018 in every environment analyzed other than e-commerce. In both cloud and POS environments, 60% of breach investigations can attribute successful social engineering as the conduit to initial point of entry. Social engineering in corporate and internal environments were slightly less yet significant at 46%. Analysis of phishing scams targeting those with authority to transfer company funds, known as business email compromise (BEC) or CEO fraud, revealed interesting results: 84% of BEC messages used free webmail services for distribution, 12% used spoofed company domains and 4% elected to employ misspelled or lookalike domain names to deceive recipients.

■ **Card-not-present data most valued by cybercriminals** – Payment card data led in the types of information most coveted by cybercriminals, comprising 36% of breach incidents observed. Most notable: Card-not-present data at 25% rose 7% from the previous year largely due to increased Magecart attacks targeting e-commerce sites, while magnetic stripe data fell 11%, coming in at 11% of incidents observed in 2018. The decline in magnetic stripe data incidents can be correlated with increased global adoption of EMV chip technology designed to better protect POS systems.

■ **Marked improvements in threat response time** – The median time duration from threat intrusion to containment fell to 27 days, from 67 days in 2017, and the median time between intrusion and detection for externally detected compromises fell to 55 days, down from 83 days in 2017. Adoption of technologies such as endpoint detection and response (EDR), behavioral analytics and stronger organizational security maturity helped lead to improvements.

■ **Cryptojacking dominates web-based attacks** – A steep year-over-year increase of 1,250% was observed in cryptojacking malware, which was almost non-existent in 2017. Used to covertly place legitimate JavaScript coin miners on websites or infect carrier-grade routers, cryptojacking malware illegally mines cryptocurrency for cybercriminals using the computing resources of unsuspecting victims. In 97% of the 2,585 websites observed that were known to be compromised, the now-defunct Coinhive miner was preferred.

■ **All web applications found to be vulnerable** – For a second straight year, 100% of web applications tested possessed at least one vulnerability, with the median number of vulnerabilities rising to 15, up from 11 in 2017. Of more than 45,000 vulnerabilities discovered by Trustwave penetration testers, 80% were classified as low risk, with the remaining 20% deemed medium to critical. The most common critical weakness involved omission of Microsoft Security Update MS17-010, which fixes the ETERNALBLUE vulnerability in the Server Message Block (SMB) protocol used for local network communication.

■ **Corporate and internal networks at most risk** – 57% of the incidents investigated involved corporate and internal networks (up from 50% in 2017), followed by e-commerce environments at 27%. Incidents impacting POS systems decreased by more than half to just 9% of the total occurrences reflecting EMV use as a successful technology.

"Our 2018 findings portray a story about adaptiveness, both from a business and cybercriminal perspective," said Arthur Wong, Chief Executive Officer at Trustwave. "We are seeing the global threat landscape continue to evolve as cybercriminals deterred by advanced monitoring and detection systems go to extraordinary lengths to breach organizations by wielding new malware variants, zero-day exploits and social engineering savvy. It's becoming imperative for businesses accelerating digital transformation to implement security programs that can quickly address attack innovation and ever-changing environments through leading-edge technologies and high-level security expertise." ■

Wipro Attack: A Dent To Its Reputation?

Wipro's systems were being used to target at least a dozen customer systems

On April 16, Reuters reported that IT services major Wipro was investigating a possible hacking of some of its employee accounts, due to an advanced phishing campaign.

The Reuters story was based on the response to a query by the news agency sent to Wipro after cybersecurity blog, KrebsOnSecurity said Wipro's systems had been breached and were being used to launch attacks against some of its clients.

"We detected a potentially abnormal activity in a few employee accounts on our network due to an advanced phishing cam-

10 years
2010-2019

360+

IT decision makers will be involved in the NEXT100

90,000+ cr

of IT Budget are getting together at

INDIA's FUTURE CIOs

NEXT100

2019

Friday, 22nd November 2019

BE THERE!

For engagement opportunities, please contact:

Mahantesh Godi +91 98 80 436623, mahantesh.g@9dot9.in
Deepak Sharma +91 98 11 791110, deepak.sharma@9dot9.in
BN Raghavendra +91 98 45 381683, bn.raghavendra@9dot9.in
Shankar Adaviyar +91 9323998881, shankar.adaviyar@9dot9.in

paign," Reuters quoted Wipro statement as saying.

KrebsOnSecurity, citing anonymous sources, had said that Wipro's systems were being used to target at least a dozen customer systems.

"It appears at least 11 other companies were attacked, as evidenced from file folders found on the intruders' back-end infrastructure that were named after various Wipro clients," KrebsOnSecurity said, quoting "a source familiar with the forensic investigation at a Wipro customer."

Wipro hired an independent forensic firm to assist in the investigation even though it did not disclose to Reuters which clients, if any, had been compromised.

Later, in a follow-up blog by KrebsOnSecurity post, an interview of Wipro Chief Operating Officer Bhanu Ballapuram, Brian Krebs, the founder of KrebsOnSecurity wrote, "Ballapuram also claimed that his corporation was hit by a "zero-day attack".

But he guessed that "what Wipro means by "zero-day" is a malicious email attachment that went undetected by all commercial antivirus tools before it infected Wipro employee systems with malware."

On April 20, Sunil Varkey, ex CISO of Wipro and now CTO & Security Strategist – Middle East, Africa & Eastern Europe at Symantec, in a post in LinkedIn, put up a spirited defence of his ex-employer.

"As I understand, the current incident which is in the limelight is not a cyberattack of any catastrophic nature impacting enterprise level, though a few external parties are trying to make it that way over the last few days. No service was disrupted," Varkey wrote.

He said Wipro "gave the best possible resistance, quick identification and mitigation, collective incident response and had the boldness to face all their relevant stakeholders to provide required assurance and commitment. All of this was possible in a very complex extensive network of this size, only because they had built a robust defence control layer over the last many years; have people with the passion who know their role purpose and organizational DNA of integrity."

From the investor/client community perspective, it surely has dented Wipro's reputation... because of the way it handled communication

Could Have Been Better

As Varkey says people started writing on lessons learned and their mantras of wisdom based on the speculations in the media. Since we do not know much beyond what is reported in the media, we do not want to get into that.

Purely looking at it from the CISO's perspective, it is difficult not to agree with Varkey's no-nonsense write-up.

However, from the investor/client community perspective, it surely has dented Wipro's reputation—not so much because of the attack but the way it handled communication. A listed company would be approached by media. Just because they are not direct stakeholders, they cannot be ignored. Wipro surely could have handled it a bit better.

However, unlike some analysts' claims, we doubt if it would impact the image of India as an offshoring destination.

This is 2019, not 2005 ■

Double Scoop

Two times
the revelation

Deepak Panda

Business & IT Head,
VGM Consultants

A TECH MAGAZINE I LOVE READING

Forbes

MY PEER IN THE IT COMMUNITY

Naresh Aggarwal,
CEO, Shakambhari
Ispat & Power Limited

MY FAVORITE SPORT

Cricket

A TECH EVENT I ATTENDED RECENTLY

'Advantages of Blockchain & AI in Hospitals' organized by the Bengal Chamber of Commerce

MY FAVORITE POLITICIAN

Narendra Modi

A PLACE WHICH I WOULD LIKE TO VISIT MORE OFTEN

Dubai

Naresh Aggarwal

CEO, Shakambhari Ispat & Power Limited

MY FAVORITE ACTOR

Akshay Kumar

MY FAVORITE SINGER

Kishore Kumar

AN EMERGING TECH THAT I WOULD LIKE TO WORK ON

Artificial Intelligence (AI)

A GADGET I USE FREQUENTLY

Smartphone

MY FAVORITE DRESS

Business Suit

डिजिट
अब हिंदी में

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

digit.in
NOW IN HINDI

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

डिजिट

LAUNCHING

digit SQUAD

Here is your chance to become a Digit certified tech influencer

Benefits of Digit Squad Member

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

Apply now by scanning the QR code

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