

ITNEXT

FOR THE NEXT GENERATION OF CIOs

New Technology

Technology Champion

Language of Business

Business Outcome

Business Alignment

Business Value

Expectation Management

Business Acumen

Right Balance

People, Process, Technology

WHAT MAKES A PRACTICAL CIO ?

Sixteen CXOs define what a practical CIO should be.

Plus

Top challenges

Top emerging technologies





Block 99.9% of phishing emails.

Phishing emails have plagued corporate inboxes for years. They dupe unsuspecting employees into revealing their account information which can lead to data breaches. That's why Gmail on Google Cloud uses machine learning to block 99.9% of malicious emails from ever reaching your inbox. See how we do it at g.co/cloudsecureIN

Go make it.
We'll protect it.

The Myth of Practical CIO



You can now speak business language. Great! But what about your work? Be under no confusion—that is to use technology to create business value. How well you do that decides how good you are as a CIO.

Shyamanuja Das

The cover story in this issue is directly from the horse's mouth—15 CIOs and one CDO tell us what it means to be a practical CIO.

The big messages that are coming from them are simple—talk and understand language of business; and balance between responsibilities.

I thought that is the basic expectation from a CIO these days—whether he is a practical CIO or not.

Understanding your business, a bit of industry issues and challenges and the ability to talk in the language of business with clearly defined outcomes is what every CIO is expected to do.

But that is the hygiene; a filter. A filter has a different purpose. Unless you are up to mark in that, it will make it difficult for you to operate. Just 5-6 years back, we had many CIOs who could not do that. So, there was this need for the continuous sermonizing.

Somewhere many CIOs have assumed that it is an end by itself.

No, you did not clear your JEE by scoring 90 plus in English. You needed to score a basic minimum in English to qualify; it is your Physics-Chemistry-Math score that decided your score; your rank.

You can now speak business language. Great! But what about your work? Be under no confusion—that is to use technology to create business value. How well you do that decides how good you are as a CIO.

Today, almost all aspects of business are touched by digital technologies and there's a competitive advantage when you can do it before others. So, many businesses are proactive in their approach to technology.

Many organizations want to go out and find what new technologies are there and how they can be used to create business value for their business. That is essentially the basis of the Use Case regime. Get an interesting technology and find a use case for it in your business.

It may sound like the anti-thesis of what you have heard till now, but it is really technology first.

A practical CIO must be knowing those technologies well, and how to roll them out in his/her business to impact business metrics. For that, he/she should be proactive within the business too and should not wait for the problem to be defined to him/her.

Understanding of business and talking its languages are not the end of the journey. That is the beginning point. Unless you do that, you do not count.

It is time you tell business what can be done before they ask you ■

Content

WHAT MAKES A PRACTICAL CIO ?

Sixteen CXOs define what
a practical CIO should be.

■ COVER STORY | PAGE 08

FOR THE LATEST
TECHNOLOGY
UPDATES GO TO

ITNEXT.IN



FACEBOOK
[WWW.FACEBOOK.COM/ITNEXT9.9](http://www.facebook.com/ITNEXT9.9)



TWITTER
[HTTP://TWITTER.COM/ITNEXT_](http://twitter.com/ITNEXT_)



LINKEDIN
[HTTPS://IN.LINKEDIN.COM/PUB/IT-NEXT/68/717/301](https://in.linkedin.com/pub/IT-NEXT/68/717/301)

BIG IDEA

Will your data center handle
your next big idea?

In a connected world, IT service availability is more important than ever. EcoStruxure™ for Data Centers ensures that your physical infrastructure can quickly adapt to the demands of the cloud and the edge – so you'll be ready for the next big idea.

To know more contact us on
Toll Free – 1800 103 0011, 1800 419 4272

#WhatsYourBoldIdea

schneider-electric.co.in

Life Is On

Schneider
Electric



■ OPINION | PAGE 19-20

How To Secure Your Hybrid Cloud Environment?



■ INSIGHT | PAGE 22-23

Is There A Weak Link In Your Encryption Strategy?



■ INSIGHT | PAGE 24-26

2018: A Year Of Change For IT Security?



■ INSIGHT | PAGE 28-29

Indian Organizations Are Forerunners Of IT Maturity In APJM: Study



■ FEATURE | PAGE 32-36

The Rise and Rise of Data Breaches

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)
Senior Manager - Digital Engagement: Manan Mushtaq
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)
West: Prashant Amin (+91 98205 75282)
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



© ALL RIGHTS RESERVED: REPRODUCTION IN WHOLE OR IN PART WITHOUT WRITTEN PERMISSION FROM 9.9 GROUP PVT. LTD. (FORMERLY KNOWN AS NINE DOT NINE MEDIAWORX PVT. LTD.) IS PROHIBITED.



Cover Design:
CHARU DWIVEDI

ADVERTISER INDEX

Google	IFC
Schneider	03, 05
Bry Air Asia	IBC
Vodafone	BC



Please recycle this magazine and remove inserts before recycling

RELIABLE

Make your business operations easy and effective

Easy UPS 3S is ideal for small and medium businesses. It delivers up to 96% efficiency in double conversion mode and up to 99% efficiency in energy-saving ECO Mode.

The Easy UPS 3S is an easy choice for your business continuity.

- Exceptionally easy to install, operate, maintain, and service
- An easy to choose and use power protection solution
- A versatile, robust, competitive UPS which is easy to expand

To know more contact us on
Toll Free – 1800 103 0011, 1800 419 4272



10 – 40 kVA 3-phase UPS ideal for:

- > Small and medium businesses
- > Manufacturing facilities
- > Commercial buildings
- > Healthcare
- > Telecommunication
- > Transportation

#WhatsYourBoldIdea

schneider-electric.co.in

Life Is On

Schneider
Electric



Khizar's story is an example to young dropouts

In Pursuit of Education

NEXT100 Winner 2015 **Khizar Mohammed Momin**, Head – Technology Delivery, PMO & Innovations, Bajaj Finserv shares the adversities he faced in life and how he works towards changing lives of families in need through counselling...

"Rainbows are people whose lives are bright, shining examples for others."
– **Maya Angelou**

"Be an informed advocate and support." – **Asa Don Brown**

I have spent my early childhood in villages and very small towns. The villages were so small that every person will know every other person in the village. But these were not the places with beaches where tourists will come or the places where you can go for fishing. These were the towns and villages with minimal resources. People used to walk for miles to fetch a few gallons of drinking water, families worked together for months to grow crops and could barely make the living. For many people, getting a new shirt once in a year



was real blessing and having a pair of slippers was almost a luxury. Local shopkeepers were kind to buy eggs from their customers and in return provide edible oil or sugar. Electricity and radio were the only known forms of technology.

A few negative things were in abundance and almost overflowing. Hatred against each other, bitterness towards neighbours and dominance over women was common. Religious divide was defined with precision and unexpectedly every child, man and woman had mastered it even without a library.

A school, a bus stop, a small hospital and a *pan-chayat* stood very prominent. It looked like these infrastructures were in place ahead of its schedule



Khizar Mohammad Momin

Snapshot

Khizar Mohammed Momin is Head – Technology Delivery, PMO & Innovations at Bajaj Finserv. He is a NEXT100 Winner of 2015. He has done his Bachelors in Computer

Science from Dr. Babasaheb Ambedkar Marathwada University. His success mantra is 'lead, engage and always go beyond to set an example.'

and were creating a sense of development.

I was part of the village for a long time and had to experience the good, the bad and the unwanted, not by choice but as a compulsion. Even though the village was small, it was rigorously impacted by every social and political turmoil happening in the country. I was not competent to comprehend many aspects of the events around me. But my mind was capturing it without understanding, simply like a scanner. Memories stored in childhood were overwhelming, but with the age I could decode it all, just like an OCR. Over time, I could clearly segregate these events into illiteracy, poverty, faith, love, hatred, knowledge, ignorance, religious divide and many more. As a mere coincidence to this realization, I came to terms with my past.

The most important thing I learned is living with the past yet not to be haunted by it. What helped me in the process was education and understanding of what's around me. But education hasn't come to me as a coincidence. There were times when I felt education was irrelevant and hard to achieve. The environment around me consistently lowered my interest in it and created situations whereby I felt compelled to abandon it. Somehow, I managed to sail through life's odds.

A few years ago, I realized that there are many young, near and dear ones who are



Nurturing the youth



going through the same struggle that I went through long back. They may not be from the same village as I, but similar and worse situations prevailed in their lives. I reached out to a few of them who had abandoned education in early stages, and a few others who were on the verge of giving up their pursuit of education. Some had valid reasons and a few had none. I could easily convince many to pursue education, higher and highest, in spite of all odds. In a very few cases, financial assistance was needed. To my surprise, the response was positive. The numbers are limited but the ones who continued education are now graduates, and postgraduates. I have not kept track of their struggle but for sure know it wasn't easy for them.

Counselling was never my cup of tea, it was a raw attempt. I am cautious in my counselling approach. I reach out only to near and dear ones who know my story. It's easy to convince them because their families know me as well. I may not be an example for them but they get a sense of what can change for them, and then they decide for themselves. There are still many who are in need.

I was astounded by the outcome. After education, what these young people brought home was not money, but instead it was peace, rational thinking, compassion and hope. It is the greatest outcome of education that I have ever seen. ■

As told to Dipanjan Mitra, Team ITNEXT

*New Technology**People, Process, Technology**Business Outcome**Language of Business**Expectation Management*

WHAT MAKES A PRACTICAL CIO ?

Sixteen CXOs define what a practical CIO should be.

Plus

Top challenges

Top emerging technologies

ARE CIOs TECHNOLOGY LEADERS OR BUSINESS LEADERS OR ACTUALLY BOTH?

WHAT CHALLENGES DO THEY FACE AND WHAT SOLUTIONS ARE THEY USING TO TACKLE THEM?

WHAT EMERGING TECH ARE THEY USING?

These were some of the questions we asked CIOs and IT leaders from leading organizations. Most of them agreed that a practical CIO needs to have a good understanding of both business and technology requirements and in fact, they are more of a business enabler. Additionally, organizations

are keen on having a practical CIO who is focussed on information security, data governance and people awareness. Moreover, as per industry experts, successful CIOs are those who are good future planners, are practical and strategic in nature.

However, success doesn't come without challenges. All businesses, large, medium or small, face various challenges. It's just how quickly and efficiently you overcome those?

As highlighted by most of them, regulations and compliance issues are the most common. Also, while most of them want to go for digital transformation, finding credible

A man in a dark suit and white shirt is seen from the back, looking at a green chalkboard. The chalkboard is covered with several large, white, 3D question marks. On the left side of the board, five business-related terms are written in white cursive script: 'Business Alignment', 'Business Value', 'Business Acumen', 'Technology Champion', and 'Right Balance'.

Business Alignment

Business Value

Business Acumen

Technology Champion

Right Balance

partners can be a big challenge. Besides, organizations face key challenges in understanding and adapting to customer requirements. It is also a challenge for them to leverage and collaborating the value network, especially with industry peers. Innovation is another major area which the organizations are focussing on in order to stay ahead of the race. Most of them also pointed out the need to address issues related to talent/skill set of the team, especially, matching and updating it to changing technology and business needs.

When it came to use of emerging tech, CIOs and IT leaders from various verticals — manufacturing, banking, consulting, pharma, etc. — mentioned that Artificial Intelligence (AI), Internet of Things (IoT), Robotics and Automation are mostly in use. While on one side, organizations are using Robotic Process Automation (RPA) to minimize efficiency issues, on

the other hand, others are focussed on using AI in their audit tools to enhance performance and efficiency. Even an Appier-Forrester study, titled *Artificial Intelligence is Critical to Accelerate Digital Transformation in Asia Pacific* highlighted that India is ranked third in AI implementation in businesses across APAC and is rapidly catching up with Indonesia (ranked first) and China (ranked second).

Different industries have varied challenges and they use innovative solutions to tackle those. It's actually how they use those solutions combined with emerging tech, such as AI, IoT, Big Data, Analytics and Automation that makes them stand out from the rest of the crowd.

Here's what 16 leading CIOs and industry leaders had to say on being a practical CIO, the challenges they encounter in their business, the solutions they are implementing to address them and use of emerging tech ■

NIRITA BOSE

SVP & Head – IT, Axis Asset Management Co

Practical CIO

A practical CIO is a person who uses new kinds of technology to adapt to changes in business.

Challenges

One of the areas we are working on is digital. The biggest challenge is finding credible partners who can help us with tools, technology, etc.

Emerging Tech

As of now, we are working on a very rudimentary form of AI. We have begun to use chatbots in our technology. We use them for customer service in our call centers. The first call is answered by chatbots and then it is routed to the call centers. This has hugely increased the productivity of our call centers■



DEEPAK SHARMA

CDO, Kotak Mahindra Bank

Practical CIO

A practical CIO strikes a right balance between what needs to be done and why it needs to be done, and pick up the right choices for short, mid and long-term.

Challenges

Organizations face challenges such as agility, ability to offer multiple solutions to multiple stakeholders and ensuring the core remains stable.

The biggest challenge is how organizations can re-architect themselves and build a digital fabric, be it for transformation, for agile delivery of solution, or making a choice between on-premise to cloud or micro-service and API-based architecture.

Emerging Tech

Recently, we announced our global ABCD charter that defines our priorities, where A stands for AI-enabled applications, B for Biometric-enabled branches, C for context-enhanced customer experience and D for data-enabled design■





SUDHIR KANVINDE

VP & CIO, IL & FS Transportation Networks

Practical CIO

A practical CIO needs to understand business requirements. Expectation management is the key role for any CIO.

Challenges

We build roads and they are across various states. Most of the time, getting network at remote places is very difficult. For instance, recently in Jammu and Kashmir, we faced severe connectivity issues.

Emerging Tech

- We are already using Big Data.
- We are also exploring and analyzing use of Blockchain and expect to implement it soon.
- We are also working on safe use of connected cars ■



PARMESHWAR MENON

SVP – IT, SBI Life Insurance Co

Practical CIO

A practical CIO is one who is grounded in the company's leadership objectives, works with the leadership team in terms of defining what the next steps of the organization are, looks at costs, and evaluates models of engagement and technology that can bring value to the organization.

Challenges

One challenge is bringing down the cost of operations. Another challenge is leveraging and collaborating the value network, especially with industry peers. The third challenge is learning from the experience of customer and knowing what your organizational capabilities are.

Emerging Tech

We have tried to implement a Blockchain across industry to facilitate better collaboration with our peers as well as to bring value to our end customer and partner network.

We are also looking at massively crunching the data by having a data lake. The focus is also on IoT ■



SANJAY NARKAR

CTO, IDFC Bank

Practical CIO

A practical CIO is a person who needs to know how to deliver and participate in the business. Technology is changing at a rapid pace. He/she needs to map the business goals with the technology and at the same time, it should give a return to the business. Also, he/she should be able to differentiate between what is built and what is run and especially, focus on the built aspect.

Challenges

The talent/skill set of the team is a key challenge.

The other challenge is the huge data created in the enterprise which leads to understanding the behavior, consumption, growth and protection of the data.

The next challenge is keeping up-to-date with the security requirements imposed by regulators.

Managing the growth of the organization and time-to-market is another key challenge.

Emerging Tech

Robotic Process Automation (RPA) is one area where we are seeing big productivity gains.

We have already initiated Big Data and Data Lake projects along with AI and BI ■



ABHISHEK GUPTA

VP – IT, DishTV

Practical CIO

A practical CIO is someone who plans for the future without compromising on the present. He has to be practical as well as strategic in nature.

Challenges

The first challenge is how IT can enable the business and do it fast.

The second challenge is security of the entire IT landscape. Customer data breach is a major challenge for us these days.

Emerging Tech

Currently, we are working on various new technologies like IoT to make our business more efficient.

We are also leveraging AI to understand customer behavior, segment them better and offer solutions which are more pertinent to him/her ■



JAYANTHA PRABHU

Group CIO, Essar Group

Practical CIO

A practical CIO needs to look after people, process and technology, i.e., in a holistic manner. He/she needs to be very close to business to understand business pain points, requirements and initiatives and work accordingly to improve the growth of both revenue and business. The focus should be more on information security, data governance and people awareness.

Challenges

Improving operational efficiency and effectiveness within our business is one of the challenges for which we need to take a more proactive step than a reactive step.

Collaborating with the right partner and understanding and implementing right technology to address business issues are very important in current times.

Emerging Tech

There are lots of initiatives going on at group level with regards to IoT, Blockchain, Big Data, AI and Mobility. This is all done with a view to providing seamless experience to both our internal and external customers■



ASHOK JADE

CIO, Shalimar Paints

Practical CIO

A practical CIO is someone who is more aligned to the business rather than technology alone. He/she looks at how technology can leverage business benefits, enhance market share, revenue growth, etc.

Challenges

Innovation in the paint industry has not really happened.

Many companies are still working with old infrastructure. Although lot of companies are using Industry 4.0, it is still not mature in the paint industry. The journey has just started.

Emerging Tech

Being a manufacturing setup, we are focussing on IoT and Machine Learning. Through this, we strive to achieve better productivity and give quality experience to our customers.

We are also using Virtual Reality (VR).

We are investing a lot in Predictive Analysis to cater to customers' varied choices of our products. So we are focussing on social media, sentiment analysis and knowing customer demands. Accordingly, we align our products and marketing strategies■

RAJEEV SEONI

CIO, E&Y India

Practical CIO

It is important for a practical CIO to apply technology to support his/her business. CIOs are now an integral part of the business.

Challenges

Regulatory restrictions pose challenges to our business and that impacts the way we structure our IT solutions, systems and support, applications we develop, etc.

Emerging Tech

When we do complex tax calculations for our clients, we are using Robotics and Data Analytics.

We are also looking at using AI in our Audit tools to enhance performance and efficiency ■



PUNEESH LAMBA

Group CIO, CK Birla Group

Practical CIO

A practical CIO is somebody who has business acumen, understands the business and has solutions to business problems.

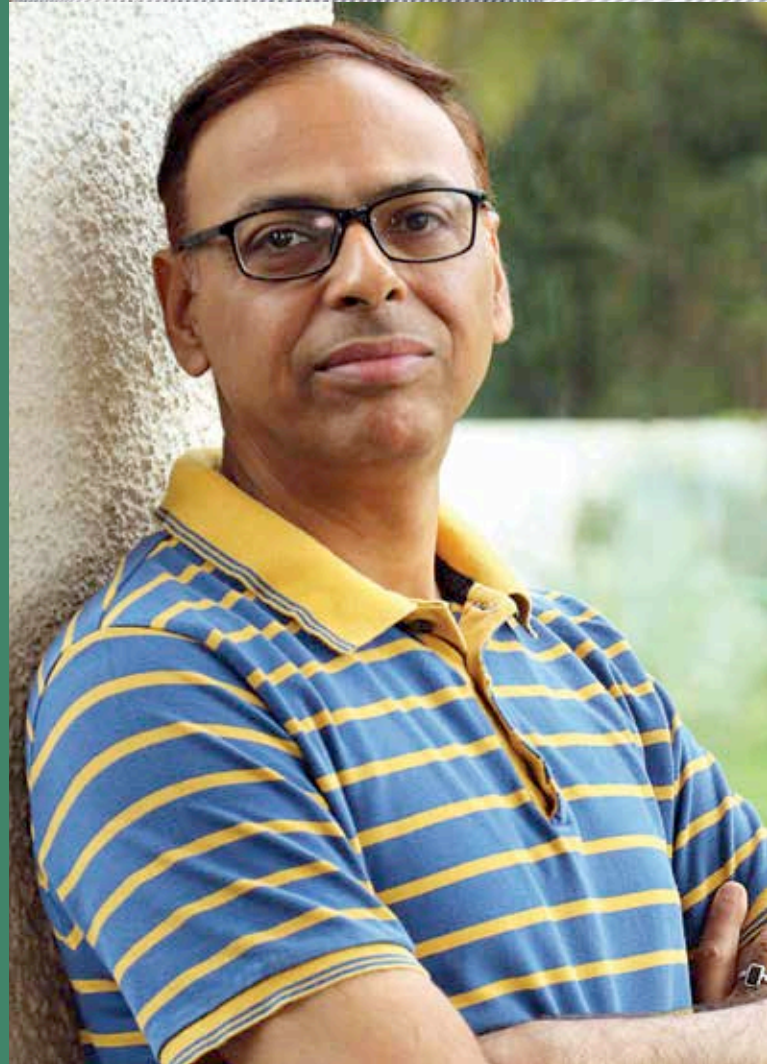
Challenges

Due to rapid technological changes, upgrading skills according to that is a challenge.

The number of vendors/partners we have in our ecosystem are not end-to-end and that is the biggest challenge that we are facing.

Emerging Tech

We are focussing on AI, IoT, Robotic Process Automation (RPA) and Predictive Analytics ■





MEENAKSHI VAJPAI

CIO, Vodafone

Practical CIO

A practical CIO is someone who is able to skilfully and successfully manage both business and technology.

Challenges

There is stiff competition and Telecom is at an inflection point in this country, and it is an extremely challenging situation. Managing unstructured and plethora of data and using it smartly to address customer pains and requirements is another key challenge.

Emerging Tech

Vodafone is a world leader when it comes to IoT. ■



YOGESH ZOPE

Group CIO, Bharat Forge

Practical CIO

A practical CIO needs to have clear business goals in mind and deliver those. He/she should have core functional domain knowledge and less external dependency.

Challenges

Processing large amount of information becomes a challenge at times.

Re-skilling employees is also challenging, but fortunately, our leadership team has been able to do that successfully.

Emerging Tech

Currently, we are using sensors and automation in our projects. We are also focussing on digitization of services. ■



GYAN PANDEY

CIO, Aurobindo Pharma

Practical CIO

A CIO today is more of a business enabler who is focussed on business outcomes rather than technology only. He/she being the technology carrier or technology champion in the organization needs to align how best he/she can achieve the business goals with right implementation of technology which can be best fitted to that IT landscape.

Challenges

Audit compliance and regulations pose a big challenge for us as we have to deal with the European and US markets—more often than not.

As investment is growing along with technology adoption, this is reducing the profit margin in the international market.

In pharma supply chain, the average inventory is more than six months. This leads to huge blockage of working capital which in turn makes cash flow really tough. So optimizing supply chain and inventory carrying costs, either at subsidiaries or distributors, especially at digital space of supply chain are a key challenge.

Emerging Tech

- We are working on predictive maintenance based on IoT.
- Some work is also happening on the AI front.
- We have also put external facing applications on the cloud.■



SACHIN JAIN

Global CIO, Evalueserve

Practical CIO

A practical CIO is one who understands the business and responds to both technology and business challenges. He/she knows how to reap the technology benefits in line with the business needs.

Challenges

At times, it becomes difficult to understand the business use cases and define a perfect score.

It also becomes difficult sometimes to understand the changing customer behavior and requirements and respond proactively and quickly.

Emerging Tech

We use various emerging tech, such as AI, Big Data, Machine Learning and Advanced Analytics to maximize on the investments we make, and the manageability and benefits the new technology brings in.■



AMIT JAOKAR

CTO, Choice International

Practical CIO

A practical CIO is someone who has hands-on experience on all the IT facets he/she is taking care of. He/she knows in and out about the domain and the business they are into.

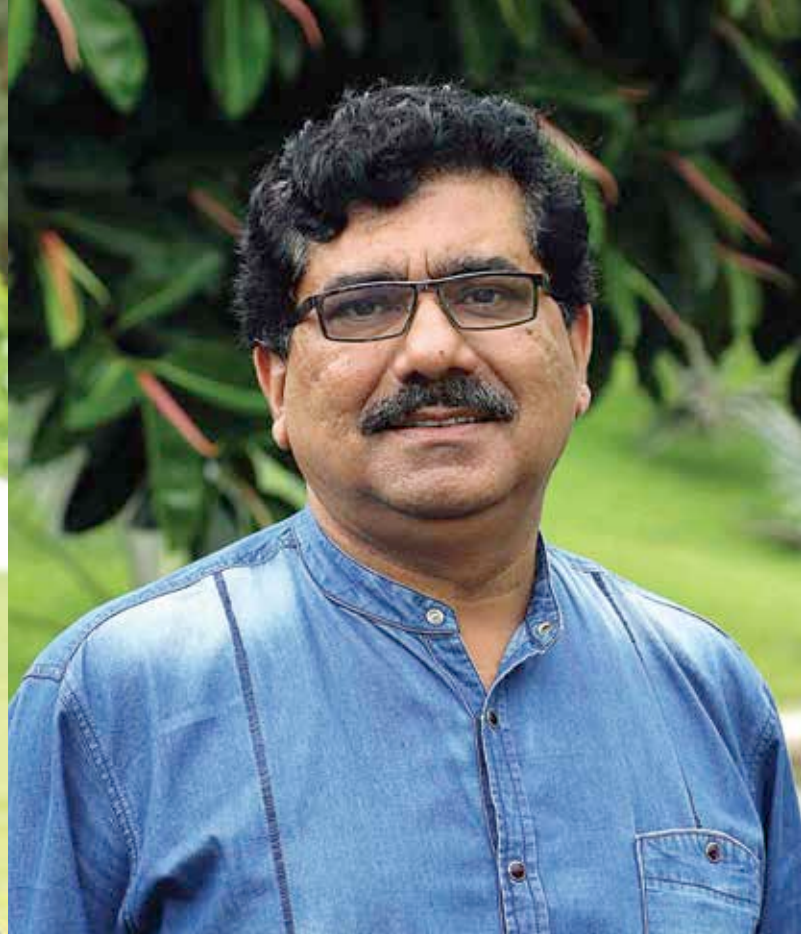
Challenges

As our major focus is on financial services, the main challenge comes when we have to deal with regulators like SEBI and RBI.

Emerging Tech

Recently, we upgraded our private cloud using hyperconverged technology. We are one of the early adopters of hyperconverged technology in India.

We are also looking out for Virtual Desktop Infrastructure (VDI) solutions, AI and IoT. ■



AJAY BAKSHI

CDO & SVP – Business Transformation, Aegis Ltd.

Practical CIO

A practical CIO is someone who does not look at technical jargon but instead works towards business solutions. However, he/she should also know how to use tech tools to solve business problems.

Challenges

The processes that our clients give are humongous, for example, preparation of large number of SLAs and adherences to be done accordingly. So the challenge is to form a balance between maintaining SLAs and adherences as well as getting the job done by the young, mobile and dynamic workforce, which has lot of potential and ability to handle customer problems.

Emerging Tech

Chatbots are one of the emerging tech we are working on.

We are also trying to use AI to ensure customers get the maximum benefits out of it.

We are also using Robotic Process Automation (RPA) to minimize some of our efficiency issues. ■



“Organizations Must Emphasize On Visibility To Stay Ahead Of Real World Threats”

In order to see the attack surface, IT security leaders have to understand the many layers that create it

By Rahul Arora

Rather than looking at the overwhelming and ever-increasing number of threats, your focus should be on identifying those that pose a real risk to your business and knowing the right patching and preventive controls to mitigate them.

To do this you need to create visibility into your assets and eco-system or what is now called as “your attack surface.” It’s time to harness the power of analytics, modeling and simulation to improve attack surface visualization. With better visibility, security teams are better prepared to fend off attacks; with the availability of comprehensive intelligence needed to build a mature security program. A sophisticated attack surface visualization solution gives CISOs and



security leaders the ability to see all security exposures at once, zoom in on problem areas and identify what’s causing the problem – all in seconds.

In order to see the attack surface, you have to understand the many layers that create it. To some, the attack surface has only been thought of in terms of vulnerabilities. But there are other factors that put an organization at risk, and they must be analyzed in connection with other attack vectors, the context of a unique network and the potential impact if they are exploited.

To holistically visualize and understand the attack surface and provide context to security risks, a solution needs to consider:

Topology: By comprehensively mapping all systems, devices and network segments as well as the paths between them, the interdependencies of your network affect risk exposures becomes more apparent. Effective solutions need to incorporate servers, endpoints, networks (including clouds), networking devices and security devices (physical and virtual) into a visual model.

Indicators of Exposure (IOEs): IOEs highlight a system, device or network that is exposed to a potential attack, helping you secure the organization before an attack occurs. IOEs include software vulnerabilities, misconfigurations and missing security controls, overly permissive rules and violations of security policies and compliance rules.

By “mapping” IOEs to an organization’s topology, security teams can quickly and intuitively extract actionable conclusions from the data. Only Skybox Horizon, an attack surface visualization tool that integrates with the Skybox Security Suite, is capable of combining an organization’s entire topology with all their IOEs in an interactive, visual model. ■

The author is Regional Director, India & SAARC at Skybox Security



How To Secure Your Hybrid Cloud Environment?

Highly-tuned ML regimes and automation identify and respond to threats with greater confidence, thereby making automated remediation a practical possibility

By Akshay Aggarwal

To keep pace with the digital economy, as enterprises race towards transforming into cloud-first businesses, the hybrid cloud environment has become commonplace. According to the *Cloud Services Market Global Report 2017* by Market Research Reports, hybrid cloud adoption has increased from 58% to 71% year-over-year in 2016.

Hybrid cloud platforms enable businesses to quickly modernize, transform and innovate. But, they also expand the risk frontier, which brings us to the question: How best can you safeguard your data as well as intellectual property across a hybrid cloud?

A continuously evolving threat milieu

Most organizations are challenged by the wide variety of threats today. As per Gartner, 60% of digital businesses are predicted to suffer major security failures by 2020. With hybrid cloud adoption on the rise, the challenge gets bigger.

The ubiquity of mobile internet (thanks to the proliferation of smart devices), along with a rising remote worker base, have together stretched the network perimeter to the limit. Now, hybrid cloud models are further accelerating this trend, compelling security practitioners to relook at the periphery - of where the secure network begins and ends.

Further, with agile development and DevOps, applications and workloads typically run in parallel, from a range of on-premises, private and public cloud databases, and get constantly updated; each one provided by a different vendor, possibly located across the globe. Given this, securing cloud services with disparate, traditional tools and practices has become unviable, also compounded by the need for integration and management of several different security products. Practically speaking, this is not only an inefficient and less successful approach, but is also error-prone.

In such a challenging environment, how can a security team make sure that its corporate security policies and

industry regulations are in place and for good effect?

The rise of hybrid cloud

What are the two key challenges you face when securing your business in a hybrid cloud environment?

Businesses require total visibility of all workloads and user activity across the entire hybrid cloud environment—spanning on-premises, cloud services (XaaS) and also unsanctioned ‘shadow IT’ environments.

Businesses need a mechanism to process and analyze the massive amount of telemetry and other data this expansive IT estate will generate, often with a flat budget and no additional resources.

In summary, organizations require a holistic/unified, complete set of data with less human effort to interact with and analyze.

The cloud is calling, where are you?

Thankfully, cloud offers a solution. New cloud services come with the ability to ingest massive amounts of operational and security telemetry, analyze the same in real time using purpose-built machine learning (ML) algorithms and react to findings using automation. These services provide for a step-function improvement in core security operations centre (SOC) functions, spanning security information and event management (SIEM), user and entity behavior analytics (UEBA), cloud access security brokers (CASB) and configuration and compliance management—also factoring in the context of identity for user activity.

Developing at cloud-scale has enabled security providers to deliver a big-data platform that spans SIEM, UEBA, CASB, compliance and context-based identity, thereby streamlining the information continuum, that was erstwhile available only in separate tranches (i.e. if it was available to an SOC team in the first place!). Highly-tuned ML regimes and automation identify and respond to threats with greater confidence, thereby making



As per Gartner, 60% of digital businesses are predicted to suffer major security failures by 2020

automated remediation a practical possibility. This inclusion of purpose-built ML dramatically improves security and allows for the creation of a solution designed to proactively identify issues or draw your attention to aspects you never considered earlier.

With such a next-generation approach, highly-skilled SOC analysts can switch focus from rote identification of routine issues to protecting the organization against the sophisticated advanced persistent threats (APTs) prevalent today. This unified approach can also enable a critical control point for use of hybrid cloud, facilitating easy visibility of cloud services across multiple solution providers as well as on-premises IT. This saves significant time and reduces human error as organizations continually rebalance workloads across their sprawling IT estate.

Before deciding on a next-generation security solution, check out if it enables the below four security func-

tions to scale seamlessly:

End-to-end visibility of the hybrid IT estate:

All workloads are made transparent, no matter where they are in the distributed, hybrid estate. This helps overcome the key challenge of our modern non-perimeter world—allowing visibility into all cloud environments in use including the unofficial, unsanctioned ones.

Strong compliance mechanism:

Configuration management, tokenization, transaction, and activity monitoring can be implemented for compliance purposes across the entire IT estate, factoring in both industry-standard and organization-specific rule sets.

Identification/Detection: A next-generation SIEM with UEBA, CASB feeds and identity context up-levels the capabilities of the SOC to detect suspicious or malicious activities, and detect risky user behaviors before the occurrence of a breach.

A system with automated remediation: Most organizations don't fully leverage automation because they lack confidence in their analytical conclusions. With ML powered conclusions, automated response becomes more trusted and a higher-percentage of SOC action, increasing overall SOC efficiency in time to counter increased set of threats.

Given the added complexity involved in managing a hybrid cloud environment, businesses require more sophisticated capabilities to protect the entire cloud/IT footprint and preempt security gaps. Solution providers are responding with next-generation solutions that unify data and apply purpose-built ML.

As India moves towards transforming into a digital, knowledge-based economy, Indian businesses must develop a more holistic, proactive approach to IT security. As Aristotle said, ‘well-begun is half done’. In today's diverse threat landscape, businesses can move towards IT security maturity by deploying the right solution. ■



The author is Director and Solution Specialist at Oracle India

Digital Transformation: The Serious Textbook For IT Managers

The book will fulfill the need of a good text book for the IT practitioners of digital transformation

By Shyamanuja Das

One of the biggest subplots of the digital transformation discourse is the debate on the CIOs' role. Is it becoming more important? Is it as important as it was a few years back? Or is it becoming irrelevant?

It is not that the debate was initiated by the digital transformation wave—it has been there for long—but for the first time, it was not IT or technology that was ruling; 'digital' had taken over—and it meant a whole lot of things. For one, technology was becoming friendlier. Then, not every technology in the organization was being channeled through the CIO and yet was making huge business impact—from cost optimization to new ways of decision making. In fact, for some, digital became a euphemism for 'saving technology from the technologists'.

This led many companies to appoint separate Chief Digital Officers—whose brief was to ensure that the entire organization—or the selected strategic priorities of the organizations—gained from the digital technologies.

And who were these new breeds of people? While in the initial phase, the marketing and technology people got into a tug-of-war to have their 'genuine' claim over the position, ultimately it is core business guys—neither marketing nor IT guys—who dominated the CDO positions.

Just for consolation, IT guys did score over the marketing people and were a distant second to business



Digital Transformation from the Trenches: Transformation Strategies for the Digital CIO
by Vivek Vishnu (July 2018)

Publishers : Authors Upfront
Pages : xviii+224
Publishers : INR 695

guys. Very few CDO positions were filled by techies. One of the few techie occupants of CDO positions in India is Vivek Vishnu, the CDO of Intex and the author of the book, *Digital Transformation from the Trenches: Transformation Strategies for the Digital CIO*.

The book is an attempt to tell his fellow techies—read enterprise IT managers—what digital transformation means for them, how they could be on top of it and how they could do it well.

The greatest advantage Vishnu has is that he exactly knows what kind of language CIOs and enterprise IT guys understand and uses that to share

his knowledge. With his own first-hand experience added, it makes for a compelling mix.

There are plenty of books on digital transformation in the market. But most of them are not written keeping the CIOs in mind. And if they have been, they clearly lack a practitioners' perspective. So, theoretically speaking, Vishnu's book has a unique proposition.

He had had the choice of writing an extremely readable book that would have subtly delivered the big messages to discerning reader but would not have been technically 'complete'. Or doing a formal, somewhat comprehensive book, that would follow a step-by-step methodological approach. He chose the latter.

Probably that was a conscious decision, because at the end what Vishnu has delivered is a very useful textbook, based on a formal methodology of his own, called DigitalCIOLIVE framework. Any practitioner who is focused on backing the disparate on-the-job learnings with a formal holistic perspective, that help him connect the dots in a meaningful manner, this would be an extremely useful book. So is it as a digital transformation textbook in MBA classes.

If your expectation is it will help you drive digital transformation in your organization, this is surely not the book. Neither is it a book for reading on your flight. You must be serious about learning to get help from the book. In short, it is for the lean-forward learner, not the lean-back casual reader. ■



Is There A Weak Link In Your Encryption Strategy?

There is little to no push from leadership to ensure there is a universal encryption policy over the entire network. Without this overarching encryption solution with centralized key management, businesses create weak links in their armour

By Luke Brown

Rather like the never-ending pool of news stories about Brexit, many of us have tuned out of reports about data breaches – whether criminally motivated or human error – simply because they're so common. We've become accustomed to stories about customers' sensitive data being lost. It's become part of the fabric of our lives. It's no longer news. IT security teams are doing their best to protect themselves from cyber criminals, constantly playing a cat and mouse catch up game.

A key part of their armoury is encryption. Almost as old as the Internet itself, it's a fundamental point of defense in preventing against dataleaks. It's a time-

tested tool that can severely hinder attackers in their goal to steal confidential user and customer data, trade secrets, and more. However, the rise of new technologies such as mobility, cloud and virtualization combined with an increasingly complex regulatory environment means companies are finding the need for encryption more than ever before. To make this worse, boardrooms are not adapting to these developments. As it is, encryption is being seen by IT operations as a tick box exercise, with point solutions encrypting only segments of network infrastructure.

There is little to no push from leadership to ensure there is a universal encryption policy over the entire network. Without this overarching encryption solution with centralized key management, businesses create weak links in their armour.

Weak link # 1 – Data Sprawl

What you don't know can hurt you. With the dissolving network perimeter, your data can be anywhere. Mobile devices and inexpensive, easy-to-use, cloud file-sharing services make it easy to work anywhere and anytime. Such access has become essential to operating in an always-connected world.

However, continuous encryption can be complicated to implement in modern environments where infrastructure and data span both cloud and on-premises servers. Native encryption technologies are useful at one level, but they can still leave your devices vulnerable, and IT admin teams are left with lots of encryption keys to juggle which is a real headache. Where companies lack strict security and encryption management for technologies such as virtual machines and hyper-converged infrastructure, uncontrolled data sprawl can be common, leading to silos of hidden data and a fragmentation of governance.

Weak link # 2 – Compliance Requirements

We know that data leaks occur

throughout the IT equipment spectrum – on networks when information is transferred or when devices are left unattended, lost or stolen and eventually fall into the wrong hands. There are lots of ways to lose information and every one of them is potentially damaging to an enterprise. With ever more stringent regulations, it's easy for an organization to fall foul of the requirements (often without knowing), leaving themselves exposed and non-compliant, and at risk of heavy fines.

Added to that, more and more regulations stipulate the need to not only protect data with encryption, but also protect the keys used to encrypt the data. In fact, GDPR, MiFID II, PCIDSS and other breach notification laws state that businesses must document and implement procedures to protect keys used to secure data against disclosure. At the end of the day, the value of encryption is only as good as the trust in your keys.

Strengthening that chink in the armour

It's easy to see how things can quickly get very complex, and why it's important that organizations enforce encryption automatically through their security policy to help avoid disaster. With boardroom enforced encryption platforms, businesses can rest easy knowing that data is protected across the network and can't be turned off by employees looking to optimize device performance, which is a real problem for both point encryption solutions



With boardroom enforced encryption platforms, businesses can rest easy knowing that data is protected across the network and can't be turned off by employees...

and anti-virus products.

Encryption not only turns information or data into an unbreakable, unreadable code should someone unauthorized try to access it, but it is also often the only technology referenced in these evolving and escalating regulations as a reasonable and appropriate security measure.

Furthermore, centralizing encryption management and ensuring keys are controlled from one point helps a company further enforce these regulatory and governance requirements. Ultimately encryption is the last line of defense when a breach occurs, regardless of whatever action caused it, invader or accident.

In Conclusion

If there is one absolute truth in business, it's that data is now everywhere. Big or small, companies wrestle with keeping data secure with an ever expanding mobile and agile workforce. Effective control and management of the IT infrastructure spanning on-premises and cloud service providers for security and specifically encryption, is the only way to minimize the risks of data loss and meet growing legislative requirements. ■

The author is Director and Solution Specialist at Oracle India



2018: A Year Of Change For IT Security?

The focus of security has shifted from a single pre-deployment event to a continuous practice, designed to detect threats as fast as possible and limit the damage

By Naveen Bhat

How will we look back on the state of security in 2018? We believe it will be seen as an inflection point – a year in which an organizations' approach to security will finally shift to being more in step with our always-on digital society. A new model of IT security is taking shape, which is more integrated with network operations, and will offer greater value to enterprises, with fewer trade-offs.

The recently-published 2018 Security

Report highlights the biggest security findings and trends from the past year, as seen and analyzed by our Application and Threat Intelligence (ATI) Research Center.

During 2018, we will see more and more organizations finalizing their cloud migrations, and moving to multiple cloud operations. As they do this, they will expect improved security as a given. But the reality is not quite so clear; cloud data breaches are up nearly 45% year over year. As enterprises are transforming their IT to embrace the cloud and mobil-

ity, security practices are not keeping pace: in fact, they are trailing behind.

Five key trends emerged from our research, and enterprises need to be aware of and respond to these trends if they are to evolve their IT security to keep pace with and protect against evolving threats.

Cloud security and compliance are priorities

The cloud is central to today's IT security landscape. Spending on cloud computing is growing, with almost all enterprises now running workloads in one or more clouds. Yet 38% of organizations have cloud users whose accounts have been compromised, and 89% of these compromises showed a marked change in users' behavior. It is no surprise that 93% of cloud IT managers are concerned about security.

Indeed, IT teams are struggling to deliver effective security in a hybrid, dynamically changing, on-demand environment. Our Security Report revealed that securing data and applications, and satisfying compliance requirements, overtook deploying and migrating applications as top public cloud priorities in 2018. The visibility gap introduced by deployments in public cloud environments is also a key concern, with 88% of our respondents experiencing issues related to a lack of visibility into public cloud data traffic.

The gap between cloud and security is growing

On average, there were over 4.3 new data breaches every day in 2017 – a nearly 45% increase from the previous year. Many of those attacks had common root causes, including unpatched vulnerabilities which allowed threat actors to compromise systems, overly permissive security policies between entities in a supply chain, and, above all, security misconfigurations allowing access to sensitive data.

In fact, one study found that nearly 73% of public cloud instances had one or more serious security miscon-

figurations. The combination of cloud growth and the high number of security misconfigurations suggests we will see more breaches where cloud is a factor in 2018. Many IT leaders are therefore turning to a multi-layer security approach to combat the challenges of an ever-expanding attack surface.

More focus needed on visibility and detection

Cyberattacks can have a severe impact on revenue as well as reputation. And yet, in the current cyber threat landscape, it is less a case of if an organization will be targeted, but when. Meanwhile, the days of securing the network purely as an on-premise challenge are over. Public cloud is

far, 2018 is the year of crypto-jacking: that is, mining crypto-currencies on devices without the owners' consent. Crypto-jacking offers cybercriminals a high-profit return that is far stealthier than a ransom attack. Code has even been found on compromised websites that can secretly transfer to users and melt down their battery powered devices. Critical IoT infrastructures are already targeted to mine digital currency. Research indicates that half a billion people are unwittingly used to mine cryptocurrency for others. As with ransomware, without a robust visibility, security and monitoring strategy to protect applications and computers, companies should not be surprised if they become the next victim of crypto-jacking.



...companies need to deploy security analysis and threat detection solutions that use granular, network packet data to identify multi-layer exploits and contain attackers

forcing a wholesale shift in security architecture to one that must encompass both public and private clouds concurrently.

As such, although critical, firewalls and intrusion prevention are not adequate to protect an organization from advanced attacks that are designed to sidestep such systems. To reduce the risk of business disruption and potential data breach, companies need to deploy security analysis and threat detection solutions that use granular, network packet data to identify multi-layer exploits and contain attackers.

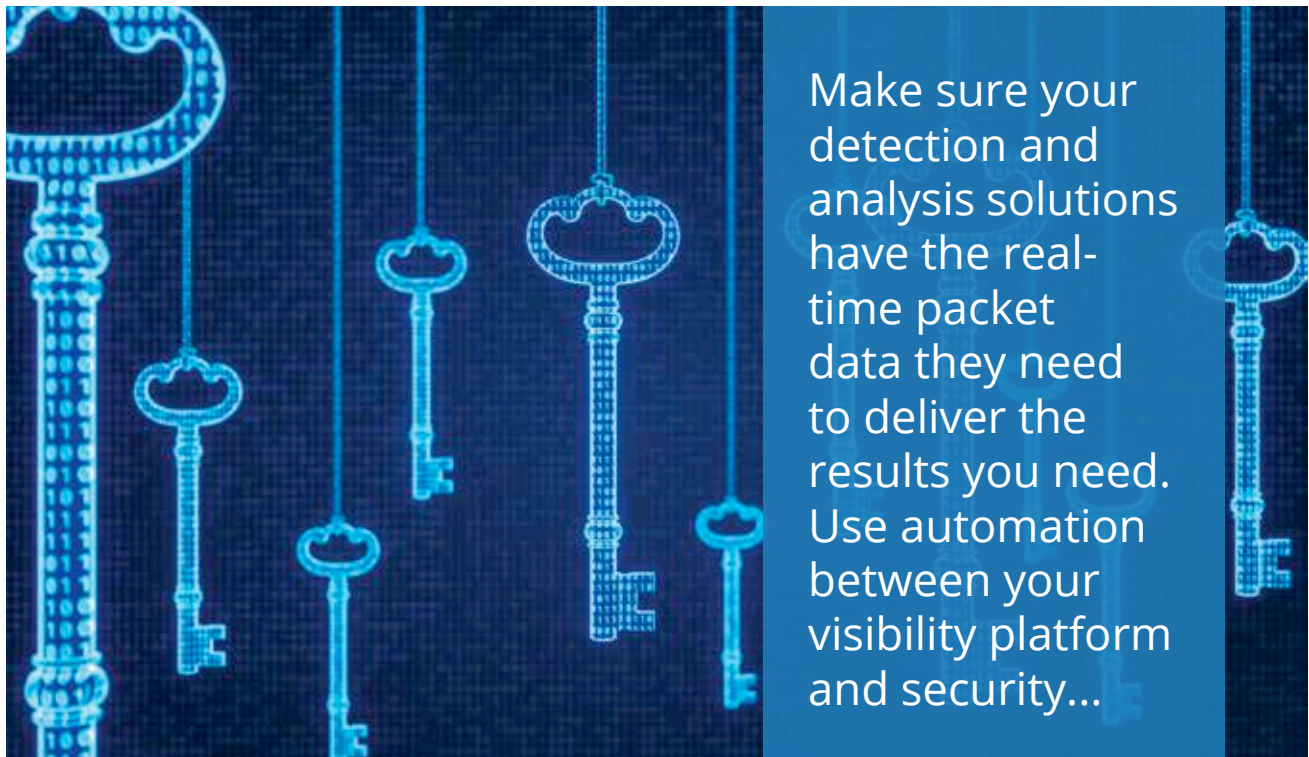
The cybercrime economy is booming

2017 was the year of ransomware. So

Encryption is good for business, and for hackers, too

A significant Internet milestone was passed in February 2017, when it was reported that approximately 50% of all web traffic was encrypted using HTTPS. This protects users – but it can also be exploited by hackers, who can hide malicious traffic in encrypted streams. This makes detection of malware or abnormal traffic via traditional means impossible and demands a complete visibility approach that combines continuous inspection with multi-layered security tailored to the application environment.

Taking steps to improve security



Collectively, these trends highlight the urgent need for continuous visibility and layered security, to address the most urgent priorities of security and privacy in our cloud-dominated world. So how should organizations react to these emerging security trends, to cut their exposure to risk and shrink their attack profile? Here are our recommendations:

■ **Visibility matters:** Security is dependent on total network visibility. Do not lose sight of the foundation of security monitoring: 'You can't protect what you can't see.' As network complexity grows, your visibility of traffic needs to keep pace. Work to understand how blind spots develop and how to eliminate them.

■ **Make resilient security your goal:** The focus of security has shifted from a single pre-deployment event to a continuous practice, designed to detect threats as fast as possible and limit the damage. Make sure your detection and analysis solutions have the real-time packet data they need to deliver the results you need. Use automation between your visibility

platform and security solutions, to enable near real-time reactions.

■ **Seeing into every cloud:**

Remember that cloud providers are only responsible for securing their physical infrastructure, and not your data or applications. Take responsibility for securing these by gaining visibility of packet-level data and performing realistic testing of all your cloud environments.

■ **Test proactively to reduce risk:**

Testing gives you the insight needed to understand how your security infra-

structure reacts under attack, so you can address weaknesses and accelerate recovery from incidents.

■ **See into decrypted traffic:**

Ensure your visibility platform supports ephemeral key decryption. Secure traffic is the de-facto standard for internet communication and transactions but can also hide threats – so ensure that you can decrypt and inspect secure traffic encrypted with ephemeral keys to expose any threats that may be otherwise hidden.

■ **Train, and train again:** Effective cybersecurity teams must have access to a rigorous training and practice environment that features scalable real-world traffic and current attacks. A high-performance cyber training program needs to constantly integrate new scenarios and attack elements to build the 'muscle memory' that is needed in real-life situations. As the US Marines saying puts it: "Improvize, adapt, overcome"■



The author is Managing Director, APAC, Ixia

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 घटनाओं से अवगत रखेगी। साथ में नए हिंदी वेबसाइट पर आपको डिजिट टेस्ट लैब से विस्तृत गैजेट रिव्यू से लेकर टेक सुझाव मिलेंगे। डिजिट जल्द ही और भी अन्य भारतीय भाषाओं में उपलब्ध होगा।

di9it.in
NOW IN HINDI



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

डिजिट



Indian Organizations Are Forerunners Of IT Maturity In APJM: Study

90% of Indian respondents agree that failing to embrace IT transformation will hurt their company's competitiveness

IT Transformation can result in bottom-line benefits that drive business differentiation, innovation and growth, according to ESG IT Transformation Maturity Curve India Report commissioned by Dell EMC and Intel Corporation.

Today's business landscape in India is rife with disruption, much of it driven by organizations using technology in new or innovative ways. In order to survive and thrive in today's digital world, businesses are implementing

new technologies, processes and skill sets to best address changing customer needs. A fundamental first step to this change is transforming IT, to help organizations bring products to market faster, remain competitive and drive innovation. According to the study:

- 90% of Indian respondents agree that failing to embrace IT Transformation will hurt their company's competitiveness
- Respondents from Transformed

organizations in India were 1.35 times more likely to have exceeded their revenue targets (97%) in the past year compared with Legacy/ Emerging Indian organizations, as compared to only 45% of respondents at Transformed companies in the rest of Asia

- Transformed organizations in India are 11x more likely to believe they are in a very strong competitive business position compared to lower scoring organizations

The ESG 2018 IT Transformation Maturity Study

The ESG 2018 IT Transformation Maturity Study follows the seminal study commissioned by Dell EMC, the ESG 2017 IT Transformation Maturity Study, and was designed to provide insight into the state of IT Transformation, the business benefits fully transformed companies experience, and the role critical technologies have in an IT Transformation. ESG employed a research-based, data-driven maturity model to identify different stages of IT Transformation progress and determine the degree to which global organizations have achieved those different stages, based on their responses to questions about their organizations' adoption of modernized data center technologies, automated IT processes and transformed organizational dynamics.

This year's 400 participating organizations from India were segmented into the same IT Transformation maturity stages:

- **Stage 1 – Legacy (2%):** Falls short on many – if not all – of the dimensions of IT Transformation in the ESG study

- **Stage 2 – Emerging (21%):** Showing progress in IT Transformation but having minimal deployment of modern data center technologies

- **Stage 3 – Evolving (61%):** Showing commitment to IT Transformation and having a moderate deployment of modern data center technologies and IT delivery methods

- **Stage 4 – Transformed (17%):** Furthest along in IT Transformation initiatives

This year's findings show organizations are progressing in IT maturity and generally believe transformation is a strategic imperative.

- 72% of Indian respondents whose organizations have achieved Transformed status also report having mature Digital Transformation projects underway versus only 3% of the Indian Legacy/Emerging companies surveyed

- IT groups at Transformed com-

panies in India are 6.5 times more likely to be involved in business-strategy development compared with their counterparts at Legacy/Emerging companies (46% versus 7%). Moreover, in the rest of the region Transformed organizations were only 5 times as likely to enjoy this level of involvement compared to lower scoring organizations

IT Transformation maturity can accelerate innovation, drive growth, increase IT efficiency and reduce cost. More specifically:

- Two-fifths (41%) of respondents at Transformed companies cited cost reduction as a key IT success criterion

- Nearly universally, 89% of Indian respondents said their companies are under pressure to deliver products and services faster, which requires having an agile approach to IT

- Transformed organizations in India were 10 times more likely than Legacy/Emerging organizations to report the majority of their applications are deployed ahead of schedule

Maturity Characteristics Compared with the Rest of Asia

For Indian organizations, IT Transformation correlates with improved IT and business outcomes.

India's organizations were more likely to report extensive (29% versus 7%) self-service infrastructure provisioning capabilities to end-users...

In terms of modern datacenter technology usage, Indian organizations appear to lead their counterparts across the rest of Asia:

- They are more apt to use Flash, 84% of surveyed Indian companies use All-Flash and/or hybrid arrays compared with 73% for the rest of Asia

- 82% of Indian organizations surveyed use scale-out storage versus 65% for the rest of Asia

- They are much more likely to be committed to software-defined data-center technologies, e.g., software-defined networking and storage—72% of Indian respondents indicated such a commitment compared with 53% across the rest of Asia

- They were more likely to report using both converged and hyper-converged infrastructure in their environments—46% versus the 19% reported by organizations in other Asian countries

- Indian organizations are more virtualized than other Asian organizations—49% of Indian production servers are VMs versus 45% in the rest of Asia

In addition to modern datacenter technologies, Indian organizations are, in general, exceeding the rest of Asia in terms of automation and process evolution:

- India's organizations were more likely to report extensive (29% versus 7%) self-service infrastructure provisioning capabilities to end-users compared with the rest of Asia

- India-based organizations are more likely to have highly automated server environments including provisioning (35% versus 15%), updating (39% versus 16%), and troubleshooting (34% versus 13%) processes.

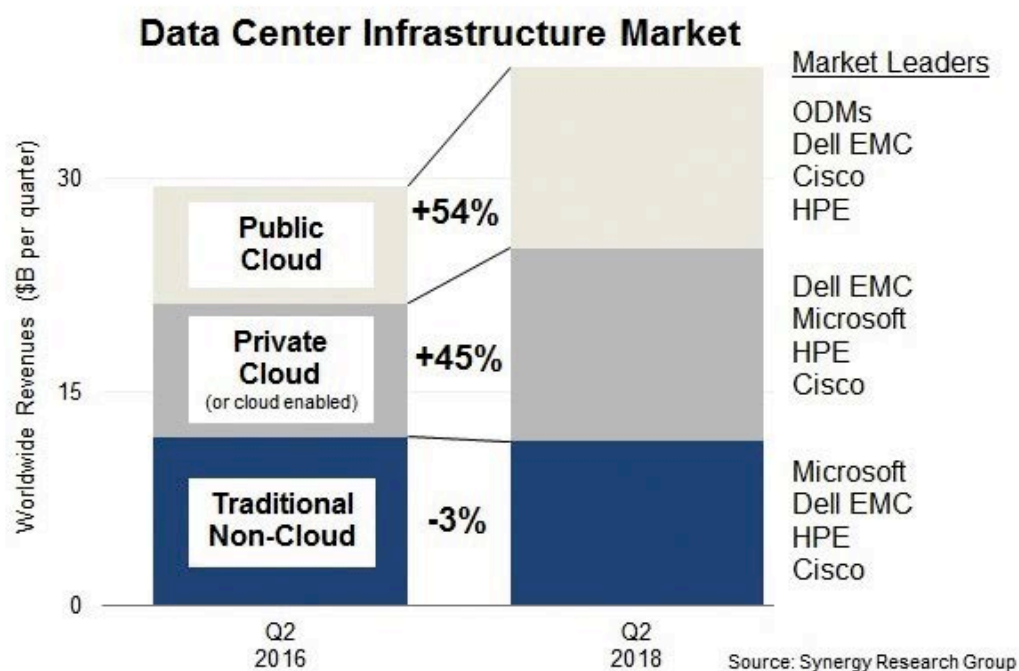
Lastly, ESG asked respondents to qualitatively describe how extensively their organizations have adopted formal DevOps principles and practices. Indian organizations appear to be ahead of the rest of Asia, with 26% reporting extensive adoption compared to 10%■



Public Cloud And Enterprise Servers Boost Datacenter Infrastructure Market: Study

Over the last 24 months, quarterly spend on datacenter hardware and software has grown by 28%, driven by burgeoning demand for cloud services and increased prices for more fully featured servers

Over the last 24 months, quarterly spend on datacenter hardware and software has grown by 28%, driven by burgeoning demand for cloud services and increased prices for more fully featured servers, according to Synergy Research Group (SRG)'s new Q2 data. The main beneficiaries have been vendors supplying public cloud infrastructure, who have seen a 54% growth in revenues over the period. Growth for enterprise datacenter infrastructure has been much



lower and spending was actually in slow decline until the recent spike in server demand and pricing gave vendor revenues a boost. Within the enterprise it is private cloud infrastructure that is driving spending with a 45% increase since the second quarter of 2016. In terms of market share, ODMs in aggregate account for the largest portion of the public cloud market, with Dell EMC being the leading individual vendor, followed by Cisco and HPE. The Q2 market leader in private cloud was Dell EMC, followed by Microsoft and HPE. The same three vendors led in the non-cloud datacenter market, though with a different ranking.

Total datacenter infrastructure equipment revenues, including both cloud and non-cloud, hardware and software, were USD 38 billion in the second quarter, with public cloud infrastructure accounting for a third of the total. Private cloud or cloud-enabled infrastructure accounted for over a third of the total. Servers, OS, storage, networking and virtualization software combined accounted for 96% of

Total datacenter infrastructure equipment revenues, including both cloud and non-cloud, hardware and software, were USD 38 billion in the second quarter, with public cloud infrastructure accounting for a third of the total

the Q2 datacenter infrastructure market, with the balance comprising network security and management software. By segment, Dell EMC is the leader in both server and storage revenues, while Cisco is dominant in the networking segment. Microsoft features heavily in the rankings due to its position in server OS and virtualization applications. Outside of these three, the other leading vendors in the market are HPE, IBM, VMware, Lenovo, Huawei, Inspur and NetApp.

"We are seeing cloud service revenues continuing to grow by 50% per year, enterprise SaaS revenues

growing by over 30%, search/social networking revenues growing by over 25%, and e-commerce revenues growing by over 40%, all of which are driving big increases in spending on public cloud infrastructure," said John Dinsdale, a Chief Analyst at Synergy Research Group. "That is not a new phenomenon. But what has been different over the last three quarters is that enterprise spending on datacenter infrastructure has really jumped, driven primarily by hybrid cloud requirements, increased server functionality and higher component costs"■



The Rise and Rise of Data Breaches

Data breaches are a phenomenon the world has accepted to live with. The challenge is, how to minimize the impact

By Shyamanuja Das

Data can do magic—so we are told. When it goes to wrong hands, the black magic can have dangerous consequences. And it is happening. Whether it is health records of a prime minister of one of the most well-governed nations or highly confidential trade secrets of some of the iconic automotive brands, or the social conversations between users of the top social media platform, not to talk of the personal details of you and me, every piece of data suddenly seems highly vulnerable to exposure.

Very recently, University of Kerala saw a data breach that compromised data of several employees and pensioners. Many hundreds of people who were on the payrolls of the varsity are believed to have been contacted by scamsters,

who claimed to be officials of the State Bank of India (SBI), reported *The Hindu*.

Earlier in September, US political newsletter *Politico* reported that The US State Department suffered a breach of its unclassified email system, and the compromise exposed the personal information of some employees. After the email breach, the department convened a task force to examine the incident, the newsletter said.

On 20 July, Singapore's Health Services, SingHealth and Ministry of Communication and Information (MCI) jointly made public that about 1.5 million patients who visited SingHealth's specialist outpatient clinics and polyclinics from 1 May 2015 to 4 July 2018 have had their non-medical personal particulars illegally accessed and copied. The data taken include name, NRIC number, address, gender, race and date of birth. Information on the outpatient dispensed medicines of about 160,000 of these patients was also exfiltrated, they said in a statement.

Investigations by the Cyber Security Agency of Singapore (CSA) and Singapore's Integrated Health Information System (IHiS) have confirmed that this was a deliberate, targeted and well-planned cyberattack. It was not the work of casual hackers or criminal gangs.

On 4 July 2018, IHiS' database administrators detected unusual activity on one of SingHealth's IT databases. They acted immediately to halt the activity. IHiS investigated the incident to ascertain the nature of the activity, while putting in place additional cybersecurity precautions. On 10 July 2018, investigations confirmed that it was a cyberattack, and the Ministry of Health (MOH), SingHealth and CSA were informed. It was established that data was exfiltrated from 27 June 2018 to 4 July 2018.

The data accessed by the attackers included the health records of the

prime minister Lee Hsien Loong, who sportingly said, "I don't know what the attackers were hoping to find. Perhaps they were hunting for some dark state secret, or at least something to embarrass me. If so, they would have been disappointed."

But he has tougher task ahead than joking about his own health records. There are voices being heard that question the investment on Singapore's Smart Nation program. In Singapore, such questioning is rare. But the access of their health records by cyber criminals seems to have shaken people.

Health records seem to be a particularly favourite target of the

204, which is second in the list of industries in terms of per exposed record cost of a data breach.

But by no means is it the only industry targeted.

Even while Singapore was detecting the attack, sports goods company Adidas announced a significant data breach involving customer data of those US customers who purchased from its stores online. The compromised data include name, contact information, user name and encrypted password. Some millions of customers could have been exposed though it is not clear how many records were actually hacked.

Considering that it came right in

The per capita cost of data breach in healthcare is the highest among all industries, according to the recently released 2018 Data Breach report. At USD 408, it is almost double that of the Financial industry...

attackers. In Australia, online health services firm HealthEngine notified last month that a small group of users' data may have been improperly accessed via HealthEngine's Practice Recognition System on its website.

"Due to an error in the way the HealthEngine website operated, hidden patient feedback information within the code of the webpage was improperly accessed. This information is ordinarily not visible to users of the site," the company said in a statement. More than 59,600 patient feedback entries may have been improperly accessed.

The per capita cost of data breach in healthcare is the highest among all industries, according to the recently released 2018 Data Breach report. At USD 408, it is almost double that of the Financial industry which has a per exposed record cost of USD

the middle of FIFA World Cup ensured that even those who normally would not have noticed the news saw it.

Just a couple of days prior to Adidas announcement, another huge compromise was reported. The compromise at Exactis, a marketing firm involved a database that contained close to 340 million individual records on a publicly accessible server, unprotected by any firewall, according to a report by Wired. The company claims possessing data on 218 million individuals, including 110 million US households. Unlike most such exposures which contain generic data like name, address, email ids, Exactis database contains "more than 400 variables on a vast range of specific characteristics: whether the person smokes, their religion, whether they have dogs or cats, and interests as

varied as scuba diving and plus-size apparel.”

While not many in India—and even in the US—would have heard the name of Exactis, it works for major consumer companies and is primarily a data company.

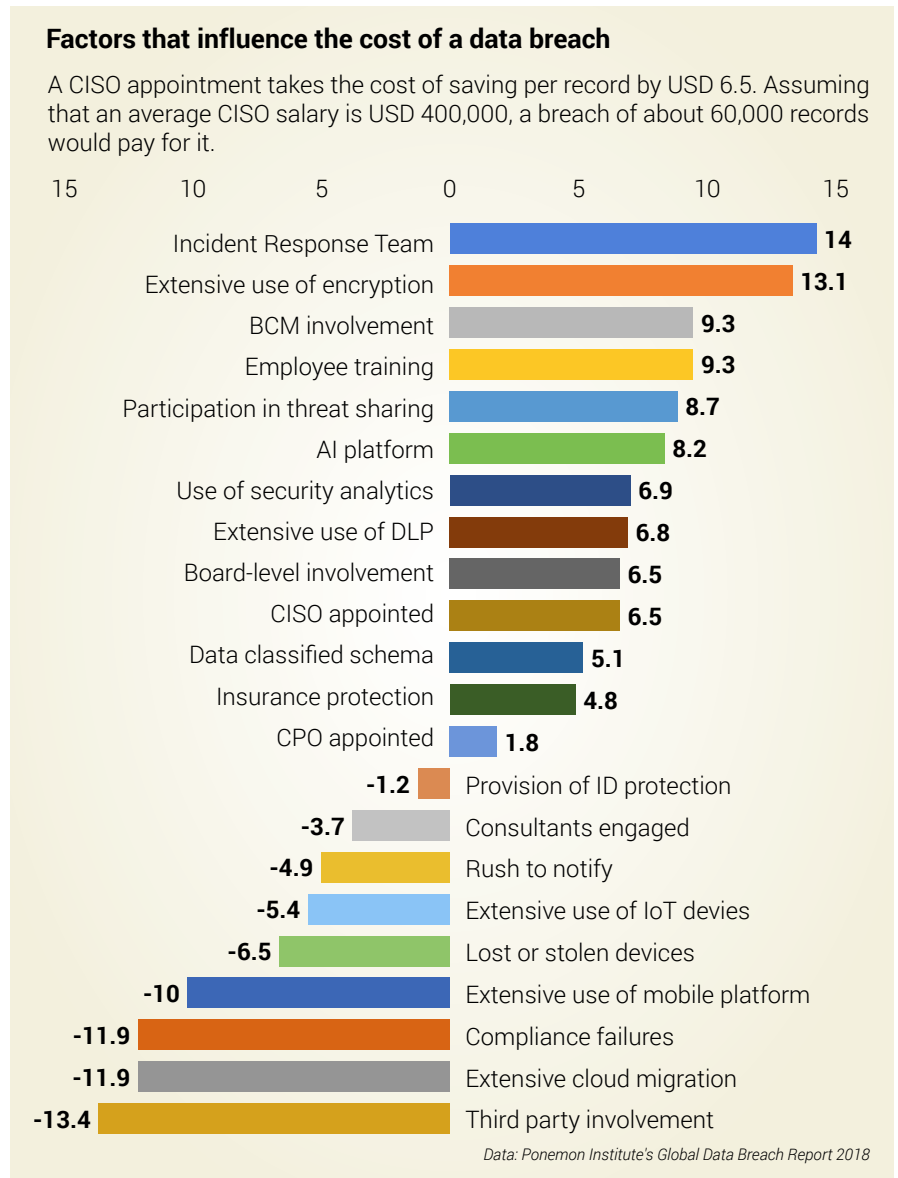
“It seems like this is a database with pretty much every US citizen in it,” Wired reported security researcher Vinny Troia as saying. Troia discovered the expose. At 340 million, it is bigger than last year’s Equifax breach which saw a compromise of 145 million records. Wired reported that while “the leak doesn’t seem to contain credit card information or Social Security numbers, it does go into minute detail for each individual listed, including phone numbers, home addresses, email addresses, and other highly personal characteristics for every name. The categories range from interests and habits to the number, age, and gender of the person’s children.”

Just like Exactis, survey firm Typeform has seen a breach that impacts consumer data of many of its clients, such as Tasmanian Electoral Commission, British prestige brand Fortnum & Mason, digital bank Monzo, and food maker Birdseye. Some of them have issued alerts to their customers but they are just a fraction of the thousands of customers that Typeform has.

The third party specialized B2B providers seem to be the weak link.

Another such provider, [24]7.Ai, which is an offshore service provider with huge operations in Bangalore (earlier called 24/7 Customer), saw its tools being infected with malware, which could have impacted hundreds of thousands of shoppers of Delta Airlines, Sears, Kmart and Best buy. Other [24]7.Ai customers include American Express, AT&T, Citi, eBay, Farmers Insurance and Hilton. Amex and Farmers clarified that they weren’t affected by the breach.

In UK, online ticket booking site Ticketmaster identified malicious software on a customer support



product hosted by Inbenta Technologies, an external third-party supplier to Ticketmaster. The company, in a statement said, less than 5% of its global customer base has been affected by this incident.

Involvement of a third party in a data breach raises the cost of the breach. According to Ponemon Institute’s 2018 Data Breach report, the per exposed record cost of a data breach increased by USD 13 to USD 161, if a third party was involved.

There are reported cases where access of data by an unauthorized party may or may not have occurred,

but the exposure of unprotected data means vulnerability of that data.

One such vulnerability was reported recently by The New York Times. It said a security researcher found ‘tens of thousands of sensitive corporate documents’ unprotected, accessible on Internet.’ Almost all major automakers such as Tesla, Toyota and Volkswagen were among the companies whose documents were found unprotected, said the report.

“Among the documents were detailed blueprints and factory schematics; client materials such as

contracts, invoices and work plans; and even dozens of nondisclosure agreements describing the sensitivity of the exposed information,” it said.

A small Canadian company, Level One Robotics and Controls, was responsible for this exposure. It is still not known if the data has been accessed by any malicious parties. But it was exposed for long.

After a Wall Street Journal report, Facebook suspended a third-party company, Crimson Hexagon, while the investigation about whether it accessed any information illegally is on. This comes after a case involving an analytics firm, Cambridge Analytica, which was alleged to use Facebook data to help political parties (including in India), among other.

Business Impact

World Economic Forum's Global Risk Report (GRR) 2018 identifies Cyberattacks and Data Theft as two of the top risk to the global economy.

But just how big is the cost to global business? Two reports give us some indication. One is, of course, Ponemon Institute's *Global Data Breach* report, referred above, which measures the cost of a data breach and the other is Gemalto's latest *Breach Level Index (2017)* which measures the universe of breaches.

According to Gemalto report, more than 4.8 million records are compromised every day. In 2017 alone, 2.6 billion records were stolen, lost or exposed worldwide. This was an 88% jump over the previous year, 2016, even though the number of incidents declined marginally (by 11%).

According to Ponemon Institute's report, average cost of a data breach in 2018 is USD 3.86 million, which is a 6.4% increase over the last year's average cost. Average cost per lost or stolen record is USD 148, up from last year's USD 141.

The average cost of data breach, of course, varies by the country. While it is highest in the US, it is lowest in Brazil. Healthcare leads all other

industries by a huge margin when it comes to per capita cost of breach. Financial and Services follow at No 2 and No 3 respectively.

Organizations undergoing a major cloud migration at the time of the breach saw this increase to per capita cost by USD 12, with an adjusted average cost of USD 160 per record, as compared to a normal average of USD 148.

The report says that a mega breach of 1 million records yields an average total cost of USD 40 million while a breach involving 50 million records yields an average total cost of USD 350 million.

To calculate the cost—the only language that businesses understand—we have to use findings from both the reports—Gemalto's and Ponemon Institute's.

Taking the 2017 data from both the reports, the global cost to business from data breaches can be calculated to be USD 367 billion in 2017, which could easily go upwards of USD 400 billion.

Businesses, though sensitized about the danger, do not yet realize the full cost of a data breach, often attaching a cost to it only if there's a financial fraud. That is a major barrier towards fighting breaches. Ponemon calculates the overall cost taking four components—detection and escalation cost, notification cost, post data breach response, and lost business cost.

Where does India Stand?

Somehow, in India, though, it is rarely that we see reports on major data breaches. Except for the Aadhaar breach, we hardly see media discussing major data breaches.

Is India bucking the trends?

Far from it. In India, breaches just do not get reported.

Recently, Indian media portal, thewire.in reported that the phone numbers, email IDs and addresses of hundreds of thousands of applicants

who took the National Eligibility and Entrance Test (NEET) in 2018 were available online. Data was available for 2.5 lakh students out of 13 lakh who took the test.

The website reported that the data was being sold at INR 2.4 lakhs for 2 lakh records. Each record contained student name, his/her NEET score, ranking, complete address, date of birth, mobile number and email ID.

The portal actually verified the claim and found that the data was correct.

However, none of the top Indian



“Perhaps they were hunting for some dark state secret, or at least something to embarrass me. If so, they would have been disappointed”
Lee Hsien Loong,
the prime minister of Singapore

newspapers has reported it.

According to the BLI Index by Gemalto, 3.24 million records were stolen, lost or exposed in India in 2017. If that seems a much smaller number—it is less than 0.25% of global records—that is because the number of consumer records online is far less.

But India is catching up. While the global number for data records compromised saw a growth of 88%, in India, that growth was 783% between 2016 and 2017. There were as many as 29 data breaches in the entire 2017 and 58% of them were identity thefts.

According to Ponemon Institute's report, the average size of data breach in terms of number of records

But India is catching up. While the global number for data records compromised saw a growth of 88%, in India, that growth was 783% between 2016 and 2017. There were as many as 29 data breaches in 2017...

compromised per breach is second highest in India, with more than 34,000 records per breach.

According to Gemalto data, of the 29 data breach incidents in India in 2017, identity theft represented the leading type of data breach,

accounting for 58% of all data breaches, the trend being similar to global trends, where 69% of all breaches were identity thefts.

Without strong regulations, companies do not report the breaches and that is the reason behind lack of coverage and public sensitivity. According the Gemalto report, the second largest global breach in 2017 occurred in India.

This involved compromise of 200 million records at the Motor Vehicle Department of Kerala. This could have been a political hot potato. But with little sensitivity about privacy, Indian political parties lack the will and understanding to highlight this.

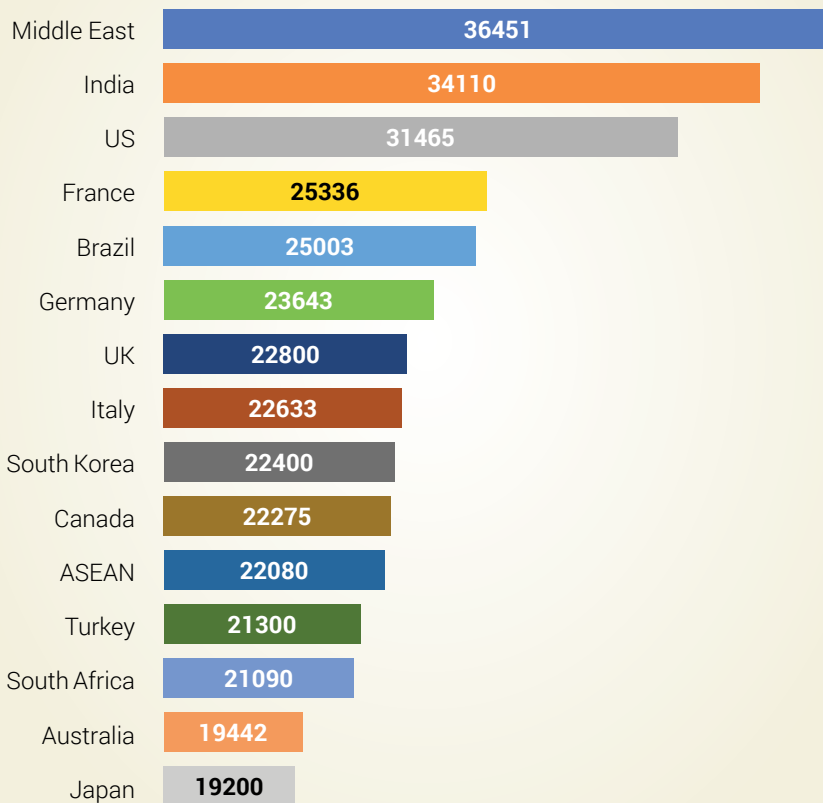
At a BLI score of 9.9 (only marginally less than the globally infamous Equifax breach which was assigned a score of 10), this was in the same league. Yet, few, even in the security community know about it.

India is working out a strong data protection legislation. A committee appointed for the purpose, is reportedly giving final touches to the draft bill. The bill is based on the feedback that it received after floating a white paper earlier. If that is anything to go by, Indian bill will also be modelled on the lines of Europe's GDPR and UK's Data Protection regulation.

India is known for producing some of the best pieces of legislation but has a poor track record of enforcement. With little awareness among people, little care by citizens for privacy and little sensitivity by media, the challenge is huge■

Average number of records compromised per breach

India is next only to Middle East in terms of number of records compromised per breach, part of which could be due to its population. But then, it is Middle East that leads



Data: Ponemon Institute's Global Data Breach Report 2018

#TheBigPicture

42% of the winners
report to a C level

64% of winners work in
organizations with IT budget
of over 10 crore and above

**Come and establish
camaraderie with the
IT giants of tomorrow**

INDIA'S FUTURE CIOs



For engagement opportunities, please contact

Mahantesh G	9880436623	mahantesh.g@9dot9.in
Deepak Sharma	9811791110	deepak.sharma@9dot9.in
Prashant Amin	9820575282	prashant.amin@9dot9.in
BN Raghavendra	98453 81683	bn.raghavendra@9dot9.in
Vandana Chauhan	9958984581	vandana.chauhan@9dot9.in

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



"IT organizations have again become popular and IT team is given a seat at the boardroom"

VC Gopalratnam, CIO for Cisco's International Operations and SVP for IT, talks to editor Shyamanuja Das on how organizational expectations from IT are changing and what that means for CIOs

By ITNEXT

Q What are the top changes that you see that have happened to enterprise IT in the past couple of years?

A About 6 or 7 years ago, when people actually started talking about digitization and digital disruption, there was a general feeling that the board would make the IT organization obsolete and the role of CIO irrelevant. But then, what has happened is that people are

recognizing that in order to do digital transformation for the enterprises, the IT organizations, and therefore the CIOs, have to play a leading role rather than just the role of enabler. Therefore, the IT organizations have again become popular and the IT team is given a seat at the boardroom. Technology is being viewed as a differentiator today for companies in order to drive the whole digital transformation or digital disruption.

As per my opinion, the digital transformation that has happened in the enterprise IT space is actually the relevance of the IT organization coming back in a serious way.

Q That is how the board thinks. What about users? Their expectations?

A The IT organization is really viewed as the service provider to the rest of the company, which

essentially means the customers (internally or externally) are demanding more and more from the IT organisation. Things need to be done in a faster, scalable and secure way.

But most importantly, the IT organization needs to be flexible, which means that the customers are expecting things to be delivered to them at their convenience – delivering the services in the fastest time with the best quality while also providing flexibility of choice.

One of the things that the enterprise IT organisation has to guard against is to make sure that what they are doing is constantly benchmarked against what is being offered outside, so that the enterprise IT organisation continues to be the service provider of the choice.

Q Earlier, business alignment was the catchphrase. Now, 'use case' which actually is an euphemism for tech-first has become the driving force. What changed?

A Honestly, the success of any organization is determined by what business outcomes they influence. For enterprise IT, the success of whatever they do is determined by the contribution to the growth, profitability of the company, deliverance of better experience for the customers, driving productivity, efficiency and the ease that we provide to our customers to do business with us. These are tangible business outcomes that are measured and if we do not influence those outcomes then we are not up to the mark.

Secondly, more business people have found their way into the IT organisation over a period of time and more IT people have moved on to the business side. Therefore, understanding of what the key levers that influence the success and failure of a business is becoming extremely relevant. One of the key skills that are demanded of IT professionals today is the ability to speak the language of business. It does not matter how smart

one is technically.

Thirdly, the technology is changing so rapidly that whether it is an enterprise platform or a mobility solution, today it is solution X, tomorrow it is solution Y and the day after it is solution Z. The technology itself is not necessarily adding the value; it is just an enabler of the value. The real value is what kind of outcomes are you delivering, whether you are influencing top line or bottom line of the company.

Q In some industries, new technologies like IoT, are

“Transformation not only means impacting the top-line growth; it means helping the business and customers become more competitive by changing the way they do business with their customers”

**VC Gopalratnam
CIO & SVP, CISCO**

giving tremendous gains. So significant is the gain that they start expanding the deployment horizontally and the organizational transformation goes for a toss. There is definitely no change in their business model...

A You can either influence the growth or profitability of the company and in some cases you can improve the productivity and efficiency of the company. Depending on the vertical, the level of impact on the top

line versus bottom line will be different. It is expected of every industry vertical to behave exactly the same. There are industries that focus quite a bit on efficiency and productivity because their margins might be lower and every rupee or dollar counts. That is where the impact on productivity and efficiency is quite significant.

Transformation not only means impacting the top-line growth; it means helping the business and customers become more competitive by changing the way they do business with their customers. Every industry vertical is different but transformation can occur in every industry as it can be related to top line enhancement or even impact on the bottom line. Therefore, it is hard to define transformation in one sentence that is universally applicable.

Q Cisco is in love with networking again. Can you explain it further for our readers?

A Digital disruption is happening everywhere. Technology is playing a very key role in this whole digital transformation. The interesting thing is there is one technology that actually is the foundation to everything. If you want to move to the cloud or if you really want to leverage data for better insights and analytics, if you want to enable IoT, if you want to put security everywhere, the one technology that makes all of this happen is 'network'. That is why Cisco believes that the network is the foundation. Clearly, the network is the first line of defence for an organisation. It is also the pathway to collaboration, productivity and digitisation. Networking enables IoT and which is why Cisco believes that fundamentally the network is more important today than it ever has been before. Cisco was founded on the principle of networking and it is why we feel honoured to fall in love with networking again. ■



Two times
the revelation



Kapil Sharma

Senior Manager – IT
Operations & Transformation
Anheuser Busch In Bev

MY FAVOURITE HOBBY

Stand-up comedy

MY PEER IN THE IT COMMUNITY



Vinothkumar Singaram

Vice President, JP Morgan Chase

A TECH TOOL WHICH I USE THE MOST

Office365



AN ONLINE SHOW WHICH I LOVE TO WATCH

TED Talks

A CELEBRITY I WOULD LIKE TO MEET

Anand Kumar (Indian
mathematician from Super 30 fame)

MY FAVORITE BOOK

Switch by Chip &
Dan Heath



MY FAVORITE SPORT

Cricket



A SONG WHICH I KEEP HUMMING

Paartha Mudhal Naale



MY FAVORITE CUISINE

Idli

MY TECH GURU

Peter Ho
(Life Coach for CEOs)



A TECH EVENT WHICH I ATTENDED RECENTLY

QlikView Forum by Qlik in Bangalore

ONE STOP SHOP

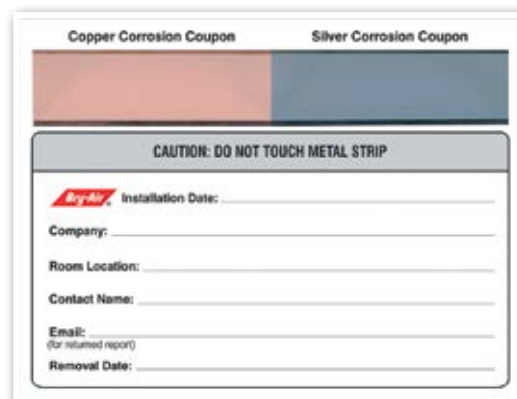
for environmental corrosion related detection and control



Atmospheric Corrosivity Monitor (ACM)

Measures and rates corrosivity level of air.
Enables you to take timely action, before the equipment breaks down.

- Gives incremental and cumulative corrosion data values
- Indicates severity of corrosion potential from G1 (mild) to GX (severe)
- Corrosion classification as per ISA 71.04-2013 standards



Corrosion Coupon



BRYSORBTM
Granular Media



DRISORBTM
Honeycomb Chemical Filters



Other Products and Services

- **Bry-Air – Gas Phase Filtration Systems**
For removing corrosive and odorous gases
- **Corrosion Coupon Testing**
For checking severity of corrosion potential
- **Residual Life**
Checking the residual life of chemical media in gas phase filtration system
- **Replacement of media, and maintenance**
Replace spent chemical of any make of GPF, and undertake upkeep of system under AMC/ AINC

Backed by
BrycareTM Service




State-of-the-art Research Lab

BRY-AIR (ASIA) PVT. LTD.

419-420, Udyog Vihar, Phase-III, Dist. Gurugram 122016, Haryana, India
Phone: +91-124-4184444 • E-mail: bryairmarketing@pahwa.com

Delhi • Chandigarh • Mumbai • Pune • Vadodara
Kolkata • Bengaluru • Hyderabad • Chennai • Kochi

www.bryair.com



**Street lamps
will know day
from night**

**Making Businesses
#SmarterWithIoT**

Global leader in IoT

The future is exciting.

Ready?



O&M 2871

To make your business smarter, visit vodafone.in/business/IoT | Call 1800 123 123 123