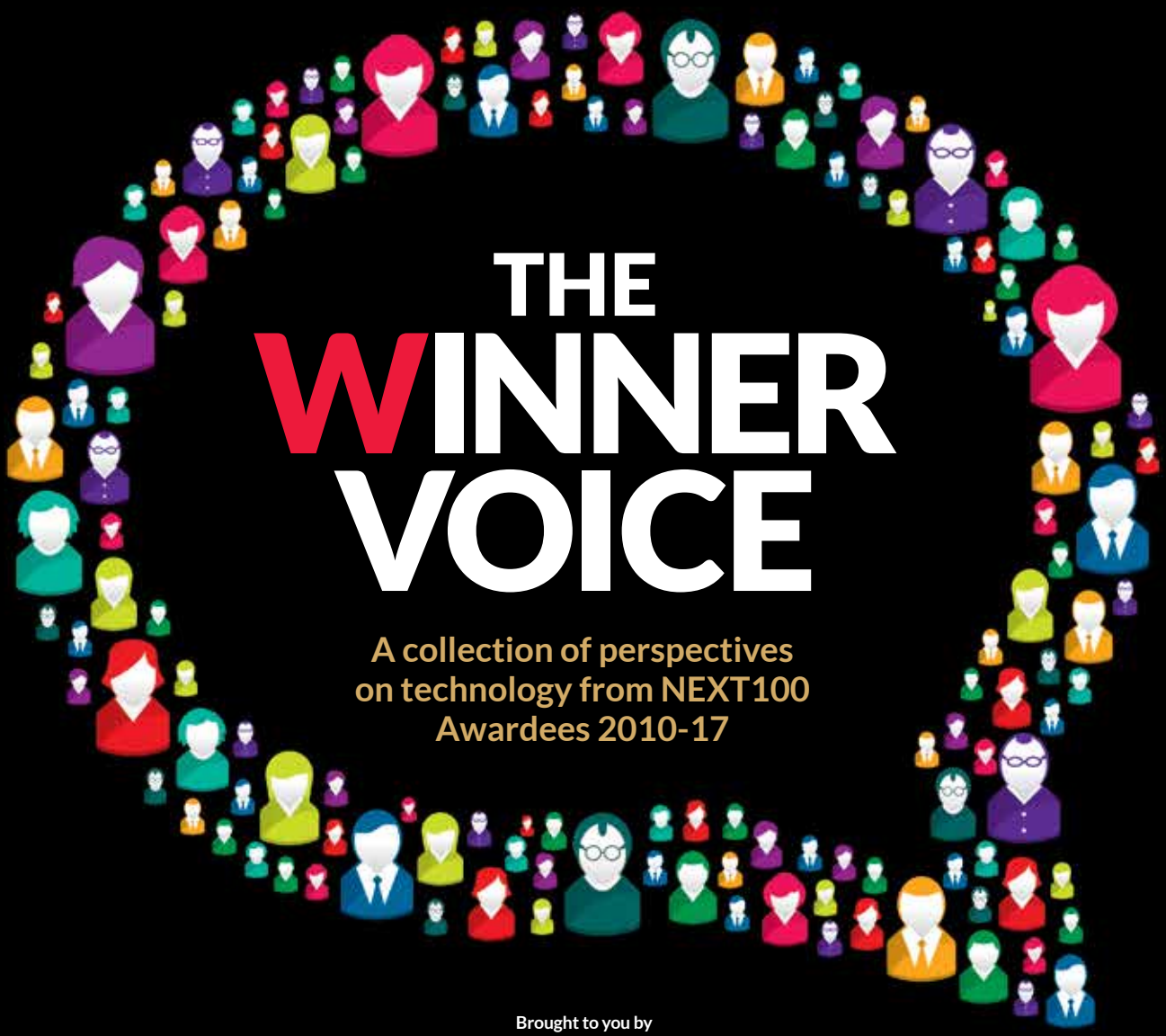
ITNEXT
FOR THE NEXT GENERATION OF CIOs
January 2018 | ₹100 | Volume 08 | Issue 09 | A 9.9 Media Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_



THE WINNER VOICE

A collection of perspectives on technology from NEXT100 Awardees 2010-17

Brought to you by

NEXT100 CLUB
WINNERS ONLY

100

Finance decision-makers of India's top companies will be getting together in March 2018

Are you there?

(WATCH THIS SPACE FOR MORE DETAILS)

For engagement opportunities, please contact
Seema Menon
seema.menon@9dot9.in, +919740394000
Mahantesh
mahantesh.g@9dot9.in, +919880436623

Tech Does Matter

When we asked NEXT100 winners to contribute their thought leadership pieces for IT Next, we had planned a single issue for that—dividing it between leadership and technology. But the sheer number of responses made us bifurcate it—one each around leadership and technology.

You have already read the Winners Perspectives on leadership in November issue. This one is dedicated to technology articles contributed by the practicing managers themselves.

Of late, there has been a popular narrative about the changing expectations from the CIO. It goes something like this. The CEO does not care about cloud and analytics; all he does is growth, profitability, shareholder value—the outcomes of the application of those technologies. A CIO, hence, must talk that language and not the language of tech.

So far so good.

But very often, this is interpreted as somewhat of a waning importance of technology knowledge, as one moves up the ladder. There are people below to understand and implement technology—the narrative goes.

That is where problem begins. Some senior IT managers are almost defensive about talking technology. A question on private cloud would elicit a response like "you know it is all about business....blahblahblah" with a liberal dosage of words like outcome, impact, business value, transformation and so on.

Yes, a CIO is expected to talk the language of business. But does it automatically mean that technology is becoming less important for him? I guess all it means is he can (or should) delegate the nuts and bolts of tech and not worry about delivery and focus on understanding strategic priorities for the business to apply the technology correctly.

If anything, now a CIO (or CDO in some organizations) is required to go out, see what new technologies are emerging and explore if and how they can create value for his business. That requires a proactive stance towards technology and an always-on-your-toes approach as technology lifecycles become much shorter. Since competitive advantage is directly accrued from enabling technologies like IoT, Big Data and Robotics, the low-risk wait-and-watch approach is no more an option. The sooner you embrace a new technology, the bigger is the competitive advantage.

That is when in the action-knowledge trade-off, knowledge becomes a little more important.

The issue that you are holding is but just a small manifestation of that shift.

Expect more in the coming months.

Since competitive advantage is directly accrued from newer enabling technologies like IoT, Big Data and Robotics, the low-risk wait-and-watch approach is no more an option.

Shyamanuja Das

JANUARY 2018
VOLUME 08 | ISSUE 09

Content

Winning Perspectives

PAGE 08-39

TECHNOLOGY VOICES

PAGE 12-15

BPM 2.0

Dinesh Tandel

PAGE 18-20

Security-In

Jayakrishnan P

PAGE 33-36

Apping IT

Sandeep Gupta

IT NEXT
ITNEXT.IN

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

EDITORIAL
Managing Editor: Shyamanuja Das
Associate Editor: Shubhra Rishi
Content Executive-Enterprise Technology: Dipanjan Mitra

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

SALES & MARKETING
Director-Community Engagement for Enterprise Technology Business: Sachin Mhashilkar (+91 99203 48755)
Brand Head: Vandana Chauhan (+91 99589 84581)
Assistant Product Manager-Digital: Manan Mushtaq
Community Manager-B2B Tech: Megha Bhardwaj
Community Manager-B2B Tech: Renuka Deopa
Associate-Enterprise Technology: Abhishek Jain
Assistant Brand Manager-B2B Tech: Mallika Khosla

Regional Sales Managers
South: Ashish Kumar (+91 9740761921)
North: Deepak Sharma (+91 9811791110)
West: Prashant Amin (+91 9820575282)

Ad co-ordination/Scheduling: Kishan Singh

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

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

OFFICE ADDRESS
Nine Dot Nine Mediaworx Pvt Ltd
121- Patparganj, Mayur Vihar, Phase - I
Near Mandir Masjid, Delhi-110091

Published, Printed and Owned by Nine Dot Nine Mediaworx Private 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

COVER Design:
MANOJ KUMAR VP

ADVERTISER INDEX	
Vodafone	BC

Please recycle this magazine and remove inserts before recycling

In this issue, NEXT100 winners, the best among India's next generation of CIOs—have put their thoughts to the keyboard

Winners on Technology

Technology is the *raison d'être* of the enterprise IT manager. Like any other business manager, an enterprise IT manager has to be a people's manager, a task manager, a project manager and wishfully, a leader. But what makes her useful for the business is her ability to add value through leveraging technology.

Yes, the role of the CIO has changed from just 'delivering' technology to 'specification to 'harnessing' technology for business value creation. As organizations embark on the irreversible path of digitalization, the expectation from CIOs is to help propel the business to new age using the best of technology available for the purpose and not look for technology to 'do a pre-defined' task.

That requires keeping pace with emerging technologies and the ability of those technologies to impact your business.

That requires you to be proactive, rather than reactive.

That's an outside-in view on leveraging technology, and not an inside-out view as it has been in the past.

That requires that technology knowledge should be pursued proactively; not on a need-to-know basis.

This issue of IT Next is an acknowledgement of the fact. This is an issue where NEXT100 winners—the best among India's next generation of CIOs—have put their thoughts to the keyboard. NEXT100, as you know, is the only program in India that identifies and honors the future CIOs. Today, some of them have already become CIOs.

What you will read in the next few pages are knowledge and its application—with a perspective that does not only come from intellectual prowess and knowledge—but also from significant experience of putting similar knowledge to practice for years. Though only a few authors have gone into implementation issues—while that was not the objective of this exercise—the experience does give them the ability to separate the 'hyped' from the 'promising'. That makes all the difference.

Though only a few authors have gone into implementation issues, **the experience does give them the ability to separate the 'hyped' from the 'promising'**

We followed a fairly simple process for this. We reached out to all the past NEXT100 winners by inviting them to write—on leadership, other management areas as well as selected technology areas.

Some of them chose to write on leadership. You have already read that in our November issue. This issue has the selected articles on technology.

Not surprisingly, most of them are about future and emerging technology. And they cover a whole spectrum—from new frameworks and approaches to trends in specific technologies; from all areas of their applications—infrastructure, security, development, and app management. And the contributors range from the first batch of awardees in 2011 to the most recent batch, i.e. 2017.

While Sandeep proposes a whole new application classification framework that would standardize infrastructure support services, Dinesh talks about how business process management should change in the era of digitalization of businesses. Jegadeeswaran actually takes a top-down view, without delving into any specific technology but instead calling out how the enterprise technology as a whole would change. While Muneesh, a recent winner talks about leveraging DevOps, as many as four of them get into security—clearly indicating what is top of mind for today. Bala goes beyond the traditional 'enterprise technology' to delve into how 5G—the new wireless technology—could help businesses.

The new expectation from the IT managers is to understand the business and be part of it. Why? In many organizations, they expect the top technology managers to tell them what is possible. This is only possible when the understanding of the business is perfect; but this also needs a very thorough understanding of the technology environment. There's nothing called 'relevant to me' technology today. Every technology is potentially relevant till you reject it. It is opt-out, not opt-in.

This issue is a small effort to help prepare you for that new paradigm. Use it for knowledge; for benchmark; or as a platform for your own thought to develop on ■



TECHN



OLOGY

We bring to you ideas that offer a solution, a suggestion, or are forward-looking in nature. The topics covered in the following pages are experiential in nature, something that some of these winners have implemented or experienced in their organizations. Turn the page to explore stories written by NEXT100 Winners on a wide-range of technology topics...

Balasubramaniam discusses the key benefits of 5G and how it will impact businesses

Hi – 5G!

Balasubramaniam Vedagiri
Senior Vice President & Chief Delivery Officer, Mphasis

NEXT100 Winner 2012

4G is a very common technology term that even technology novices are adept with, given the mobility is accessible through wireless or their operator's network. The next generation of mobile network is known as 5G or 5th Generation mobile network or 5th Generation wireless system. According to Technology Analyst TBR, 5G is a new radio technology interface that is significantly more powerful (with higher speeds, higher capacity, lower latency, etc.) than cutting edge LTE technology. It is also an era of fundamentally new architecture for the network characterized by cloud centricity, software mediation and programmable with near real time connectivity. It leverages artificial intelligence, automation and analytics to provide limitless capacity.

In order to enable individuals and enterprises with real-time and on-demand experience, 5G would provide a single network infrastructure that can meet diversified service requirements. Thus, 5G era technologies will include Network Function Virtualization (NFV), Software Defined Network (SDN) to support the underlying physical infrastructure along with Cloudification and automation. The important link to make it happen is the 5G Radio Access Network (RAN) that reside between a device like cell phone and the core network. 5G's capability to configure, scale

and reconfigure logical nodes using software codes enable RAN to dynamically adjust to changing traffic conditions, hardware faults as well as new service requirements.

Cloud-native NFV creates a new kind of distributed computing environment that has scalable, resilient and fault-tolerant features. It packs the combined surplus capacity and automated self-healing capabilities to meet any surge in consumption pattern. NFVs can help in accelerating inclusion of IMS capabilities and network security thus letting the users access computing power and data on server farms far away, rather than on their own devices.

The blueprint to Cloudify RAN is to implement the likes of Huawei's Mobile Cloud Engine (MCE) which modularizes different Network functions to deploy them across the network depending on use cases. The MCE helps flexible orchestration of RAN Real-Time and non-Real-Time processing functions based on different service requirements and close proximity to users.

5G service types can be classified into three broader categories:

Extreme Mobile Broadband (xMBB): The Internet of Things, Video surveillance and Cloud expansion initiatives will get super charged due to this service type.

Massive Machine-Type Communication (mMTC): Machine to Machine (M2M), Sensors and Augmented reality will get fillip as a result of this rollout.

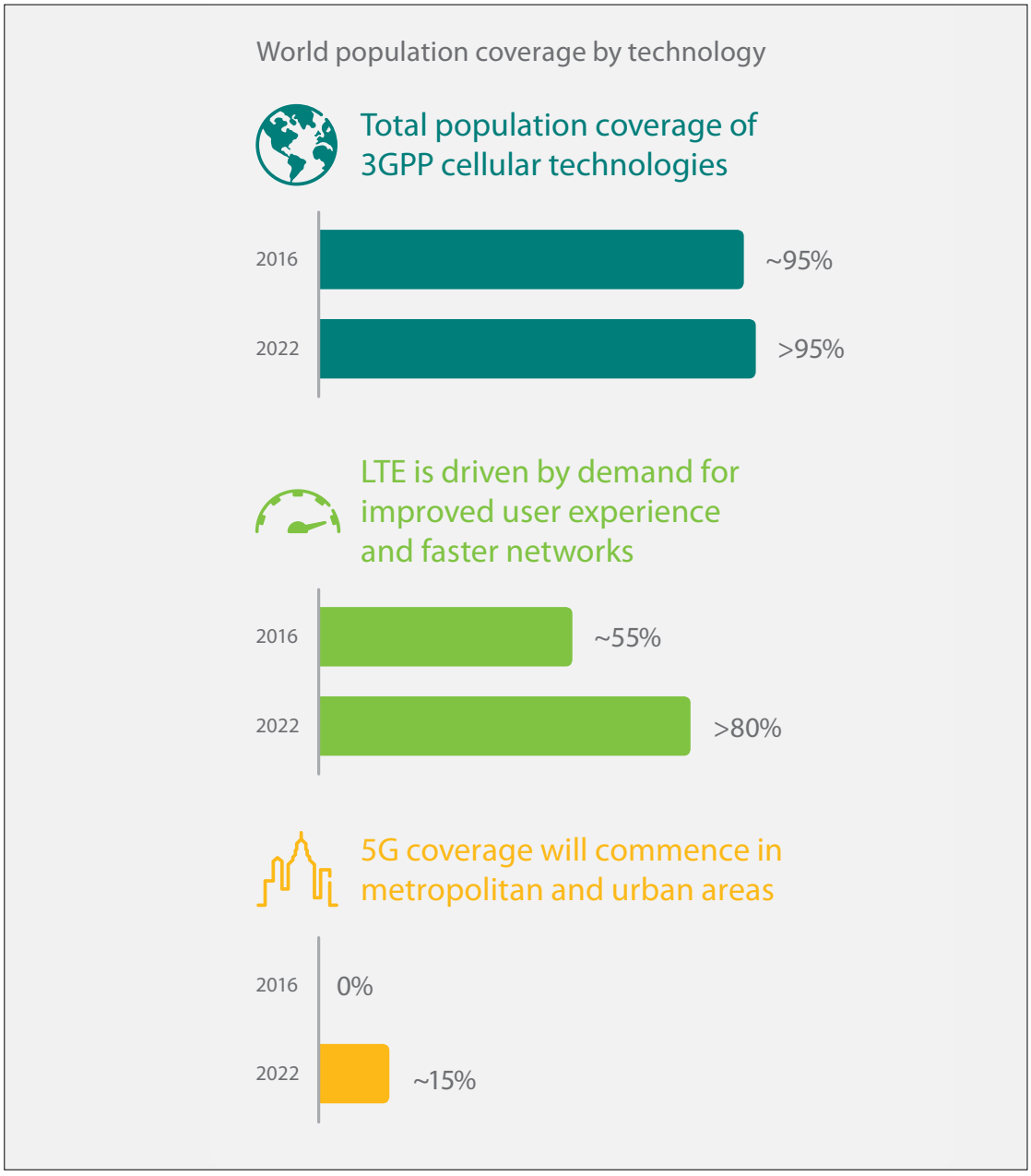
Ultra-reliable Machine-Type Communication (uMTC): Vehicle to Anything (V2X) communication that powers connected cars and industrial control applications are the outcome of this service type.

With business communication technology undergoing massive change due to this new disruption, 5G ushers in an era of reliable communication at lower cost and improved security. The mobile operators and other carriers will partner with the enterprise at large, to provide an opportunity for exponential business growth. The 5G Fixed Wireless Access (FWA) is expected to enhance productivity as huge volume of enterprise data can be transmitted in a very minimal time to any form of cloud. Since 5G should deliver the best that cloud can offer, it will pave way for proliferation of new and complex applications and services, many of which are unknown today. From existing networks enabling compute power to reside on the cloud, 5G will have an empowered application that is capable of leveraging the network to the fullest.

Eventually, 5G will not only alter cloud computing but also surround capabilities like robotics. It will aid in the development and provision of cognitive services or Cognition as a Service (CaaS). Robot sensors will soon collect the data from the environment, which will be transferred through 5G infrastructure to the cloud. With the variety of methods and techniques, the robot's intelligence will be processed remotely. APIs or Microservices will become available to the users and developers to code additional services with robots. The combination of robotics, teleoperation and cloud technologies is poised to transform industrial engineering with 5G as the singular backbone.

The Winning Tip

5G will **not only alter cloud computing but also surround capabilities** like robotics besides aiding in the development and provision of cognitive services



Source: Ericsson Mobility Report - June 2017

The core value of 5G networks can be derived only when the processing takes place from the cloud to the edge devices which is commonly referred as Fog Computing. Fog computing becomes key element of the 5G rollout with the help of small cells known as Micro-cells (also called pico and femto cells) apart from the Macro-cells which is the roof-top base stations. This makes the architecture of 5G networks a hierarchical one - with the core network (cloud) at the apex, followed by macro-cell base stations and micro-cell base stations, and finally end devices. With the assistance of the application data sent directly from one device to another, this unlocks the efficient device-to-device communication to scale up to handling numerous interacting devices.

The key benefit of 5G rollout would be capex reduction for the Telecom operators. Capex is likely to remain relatively flat or down despite ongoing data traffic growth. With the standalone 5G standards (5G NR SA) in which 5G radio and packet core operate on a stand-alone basis is expected to be finalized by mid-2018, the adoption rate is only expected to explode by end of 2018.

Let us get ready and welcome the new era of 5G mobility! ■

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

Dinesh outlines the key components of BPM and the role it plays in ensuring digital success for enterprises in the future

BPM 2.0

Disruptive technologies like IoT, robotics process automation, AI, machine learning, AR/VR, social mobile, analytics and cloud are transforming the way enterprises think and operate today. Enterprises face multiple challenges like managing global operations, increasing operational efficiency, ensuring compliance, enabling continuous automation using various technologies and responding to market dynamics.

In this customer-centric and rapidly changing world, is there any chance digital enterprises are still using Business Process Management (BPM) the way we know it? No.

There is a paradigm shift in the way applications are configured, implemented, simplified and consumed by businesses. Now is the time to think differently about BPM that drives the digitally-enabled enterprise. We need to analyze how digital transformation will influence people, processes, and systems and revise established BPM concepts in order to define, design, execute and optimize the processes. Consumers become the key to defining the way forward. Advanced BPM with low code that enables rich and complex business applications to be rapidly developed and implemented as a key enabler for business transformation will lead the way.

Dinesh Tandel
Presales Lead,
Global Solutions,
Schneider Electric

NEXT100 Winner 2011

Role of BPM in Enabling IoT

The IoT is a network of internet-connected devices able to collect and exchange data using embedded sensors. Gartner predicts in 2020, around 21 billion physical things will be connected to the internet; the estimated market size is projected to increase from USD 1.9 to USD 7.1 trillion. BPM is a vital component of any device that has IoT connectivity. IoT devices excel at sensing, alerting, augmenting reality, and generally interacting seamlessly with the wearer, but are somewhat lacking in areas such as system integration, data processing and process logic. BPM fills this gap by integrating people, processes, tools, systems and devices.

BPM's role in IoT is to determine what is to be done with data received from other devices. BPM supports time sensitive, dynamic business processes, and takes advantage of the real-time data coming out of and going back into IoT devices. Growing adoption will result in more data and more connected devices. Digitalization using BPM involves using digitized data to enable organizations to make quicker decisions, enable optimization of processes and, ease the life of users. BPM provides the ability to integrate processes that involve devices, systems, and humans. Advanced BPM solutions provide access across devices with responsive user experiences, allowing access-driven information sharing across the enterprise. It offers powerful business activity monitoring for business intelligence and actionable alerts against KPIs and thresholds.

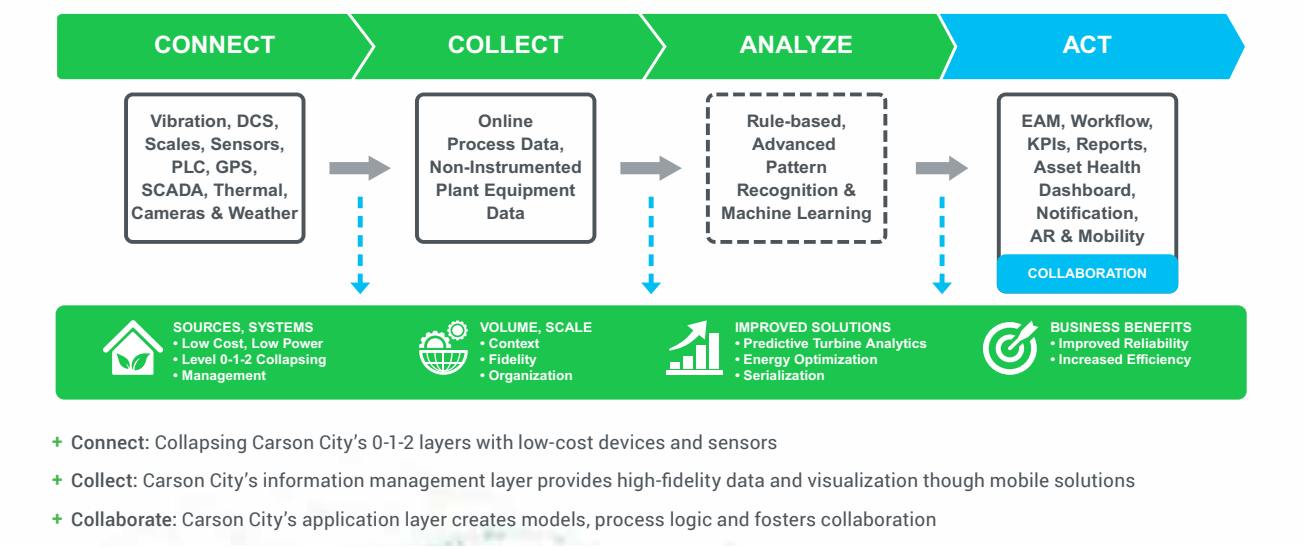
The Winning Tip

Real value to customers lies in **making meaningful business context of the data and delivering actionable information and value for the business.** BPM of things is the right choice to secure success when digitizing your business

RPA and BPM Applications: Complementary Technologies

There is a similarity between the goals of BPM and robotic process automation. The goal of BPM implementation is to increase process efficiency, improve agility, achieve better control and governance by streamlining and automating business processes. It also helps companies identify improvement areas and ensure best practices. The goal of robotic process automation is to reduce cost and headcount by providing automation of repetitive and standardized tasks. Both aim to achieve similar goals with different approaches. It's very important for enterprises to know and understand the scope or need of BPM that would provide agility and most effective return on investment. Robotic process automation and BPM are complementary technologies; combining them will result in a powerful collaboration, enabling "Intelligent Business Process Automation" resulting in a far more efficient and effective automation solution for both knowledge capture and repetitive tasks. Fundamentally, an important aspect of the assessment would be to create a business case and use these technologies to their best advantage.

In the past few years, robotic process automation has been widely adopted by BPO providers to create "virtual workforces" instead of physical workforces. This implementation was originally driven by the need to reduce costs, time, and human errors associated with employing people to work in service centers and perform routine and transactional IT-related tasks. Robotic process automation is designed to operate processes at the user interface layer. It doesn't require developers to develop interfaces and adaptors to connect to the applications and it can be easily enclosed as an API. By contrast, BPM requires web services and APIs to integrate with



Source: Wonderware BPM of Things 05-17

applications which requires a certain amount of development effort. On one hand, if you are looking for automating specific human activities mainly on structured data and relying on a surface-level fix, robotic process automation would be the right choice. On the other hand, if you are looking to transform entire existing process with complex business rules, better control and governance, then BPM would be the right choice.

Critical Components of a BPM Suite

The BPM solution for successful digital transformation comprises process, analytics, collaboration, integration, automation and flexibility to access from anywhere, at any time. Let's look at the critical components of a BPM solution and the roles that they play to secure success in digitization.

Process Engine

Essentially the core of a BPM solution, the process engine takes on the responsibility of managing all transactions, notifications, task scheduling and much more. The process engine has all the built-in technology and code of the BPM. Each business has different methods, processes and action items. The BPM process engine provides an easy approach to design, simulate and maintain these disparate processes. The process engine will act as a middle layer between the various disparate systems and applications.

The process designer that is typically user interface based enables users to drag and drop the steps or activities to create the business process. An activity is a building block for the available process; it is a reusable component available ready to use, just by configuring the relevant properties.

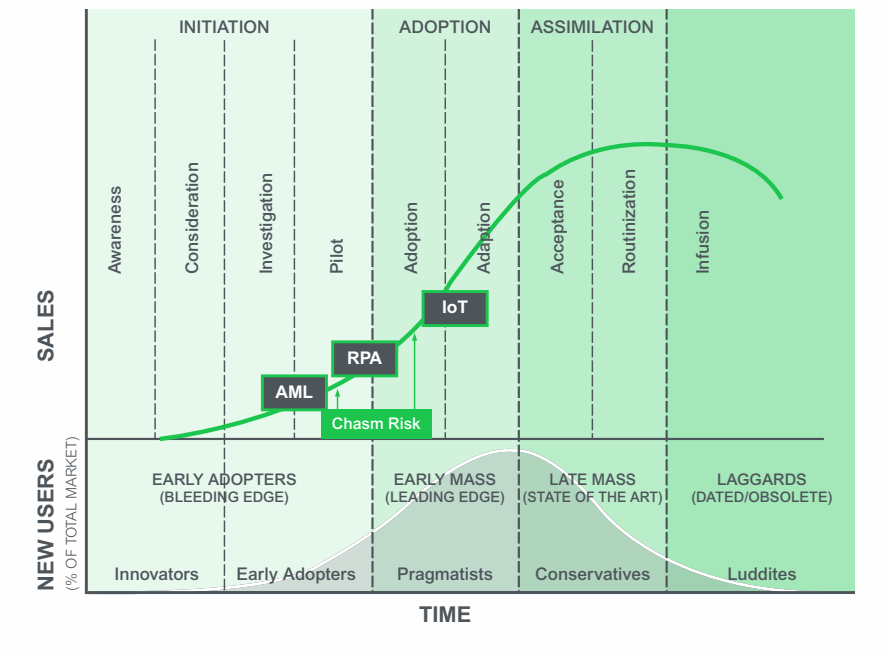
The forms designer allows users to create the UI for the said business applications. Again, drag and drop re-usable controls that make creating an user form or input form simply and easily. Multiple options of styling are available to jazz up the user interface as needed.

The task notification mechanism, unique to each BPM solution, offers different ways of communication to the users. Advanced BPM would have many delivery channels and integration options for user communication as well.

A BPM solution allows users to create enterprise level portals for the various users. The process engine captures all data with respect to the processes created. Digital evolution occurs when all the systems are brought together on a single platter, be it IoT connecting all devices or robotic process automation that uses the automated scenario for repetitive tasks.

Business Analytic Monitoring

An integral part of a BPM solution is monitoring automation, bringing into perspective the whole process. The process data captured in the BPM engine is most useful when presented in a user friendly dashboard. The data captured is made actionable because of the Business Activity Monitoring (BAM). Each process will have specific metrics that are monitored and presented such that critical business decisions can be made. Monitoring also involves performance analysis for each resource, activity state and user. KPI reports, overall bottlenecks, and status are displayed in easy readable format. BAM involves



Source: Wonderware BPM of Things 05-17

debugging of stoppage issues, online, near real time tracking for business critical decisions. BAM gives organizations powerful leverage to adapt to ever changing market dynamics.

Collaboration

The most tangible benefit of a BPM solution is the ability of the underlying technology to talk across various disparate applications and act as a single collaborative tool. This allows users access to all applications, notifications and tasks anytime anywhere in an access-controlled environment. And since each step and activity is tracked on the system, BPM offers the most secure yet collaborative user environment for business users. With digitization consumers expect updates at the tip of their finger or in their palms, on their phones, collaboration is arguably the most important benefit for the organization choosing to use a BPM solution for process automation and optimization.

Document Management System (DMS)

A BPM suite intrinsically has the capacity to maintain and process document centric processes as well as electronic forms based processes. The document management capability brings in to picture various aspects, such as version control, assess management, storage, indexing, archival and retrieval. The advantage of using a BPM suite for a document centric process is that in addition to the above said features, the full blown BPM features such as monitoring, designing and maintaining the process become easy. The BPM suite will act as a single platform for complete process automation.

With the entry of emerging, disruptive technologies like IoT, robotic process automation and advanced machine learning, the source of receiving data is changing and the way of consuming data in the business process has also changed. Now is the time to think differently and revise the established BPM concepts in order to design, automate and optimize the processes. Nevertheless, emerging technologies are in the introduction phase (as shown in Figure 2).

Companies are still experimenting and waiting to realize the benefits of these technologies whereas BPM has already made itself indispensable. BPM is seen as very strong in process automation and optimization interacting with multiple core applications/systems like ERP, SCM, CRM, PLM, MES and other third party applications along with human intervention.

IoT and BPM integration helps enterprises achieve not only cost savings but increased efficiency and improved reliability by way of real-time data collection from connected devices and consuming them through business processes. BPM solutions are comprised of process, analytics, collaboration/integration, automation and flexibility to access from anywhere, at any time ■

*The article has been co-authored by **Keith Chambers**, Director of Operations and Execution Software, Schneider Electric and **HimaBindu Gadhe**, Technical Consultant, Schneider Electric*

Dr. Rizwan discusses the challenges that IoT faces and the possible solutions needed to ensure security in IoT

Security of Things

Dr. Rizwan Ahmed
President - Technology,
QM Computech Pvt. Ltd.

NEXT100 Winner 2017

The Internet of Things (IoT) is used to describe a network of objects (or "things") that have sensors or hardware, and software to enable objects to connect to the Internet through wired and wireless networks. Early experiments conducted during the 1980s and 1990s started showcasing "things" that could be connected. The term IoT was invented in 1999, initially to promote RFID technology. IoT didn't become popular until 2010-2011. In 2011, Gartner, which invented the famous "hype-cycle for emerging technologies", included a new emerging phenomenon on its list: The Internet of Things.

In 2014, IoT reached mass markets when Google bought Nest for USD 3.2 billion and Consumer Electronics Show (CES) in Las Vegas was held under the theme of IoT. Today billions of "things" can "talk" to each other – from TVs, fridges, cars, smart meters, health monitors and wearables. As per Gartner's forecast, 8.4 billion connected things were to be in use worldwide in 2017 -- up by 31% from 2016, and will reach 20 to 30 billion by 2020, with total IoT spending on endpoints and services to reach almost USD 2 trillion in 2017.

A wide variety of IoT objects and applications are currently avail-

able, with many more to come. Here is the list of most popular IoT applications in use today:

- Smart Home
- Wearables
- Smart City
- Smart Grid
- Industrial Internet
- Connected Cars
- Connected Healthcare
- Smart Retail
- Smart Supply Chain
- Smart Farming

Technology is only adopted when it actually gets meshed with our everyday life; considering this, IoT still has a long way to go. As for the future, it is impossible to offer precise predictions as to what devices will be developed. As a paradigm, IoT should further simplify our lives by utilizing connected devices.

On one hand, IoT opens up exciting new business opportunities and a trail for economic growth. On the other hand, it also opens the door to a variety of new security threats. Since IoT involves networking of "things" or objects that are relatively new and their product design doesn't always consider security an important factor. Most of the IoT products in the market are often sold with old and unpatched embedded operating system and software. It is generally observed that purchasers of these IoT devices often fail to change the default passwords or fail to select sufficiently strong passwords.

IoT also faces a greater number of possible threats as compared to earlier internet technologies due to the various reasons:

- With ever growing number of connected IoT devices, applications, systems and end users, result in greater scope for vulnerabilities.
- Every compromised IoT device becomes a new possible attack point increasing probability of attacks.
- There is a plethora of IoT standards and protocols, which creates security blind spots. With more connected devices in many applications i.e., hundreds of different use cases build on different standards, interact with different systems and have different goals, especially critical infrastructure applications where there is a rise in the impact of attacks (i.e., damage to the physical world and possible loss-of-life), the stakes are much higher for hackers which increases the threat level.
- Due to more complex technology stack for IoT, multiple threats are possible from across the stack (e.g. hardware, communication, and software elements).
- IoT devices are collecting lots of data and this "data" can get into wrong hands, fueling privacy concerns.

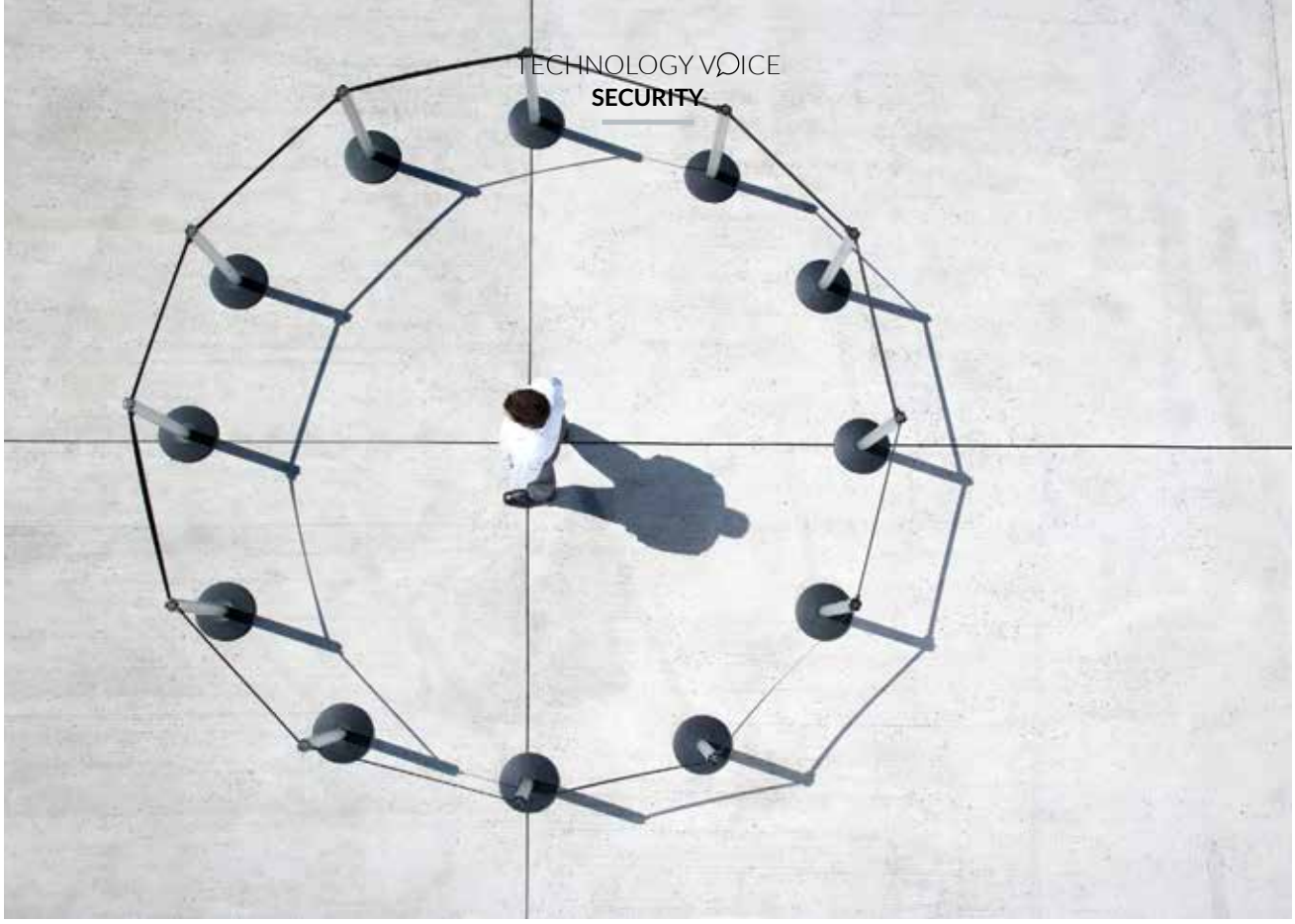
The Winning Tip

IoT security is key to **gain and retain consumer trust on privacy and fulfill the promise of IoT**

In order improve security of IoT devices, the following measures should be undertaken:

- Security must be the foundational enabler for IoT.
- IoT devices that need to be directly accessible over the Internet, should be segmented into its own network and have restricted network access. These individual network segments should be then monitored in order to identify potential anomalous traffic so as to take further action if there is a problem.
- IoT device manufacturers should enhance privacy and build secure devices by adopting a security-focused approach, reducing the amount of data collected by IoT devices, and increasing transparency and providing consumers with a choice to opt-out of data collection.
- IoT solution architectures require multi-layered security approaches that seamlessly work together to provide complete end-to-end security from device to cloud and everything in between throughout the lifecycle of the solution.
- Encryption is an absolute must.
- IoT standards are important catalysts and should further mature as per IoT security requirements.

The continued evolution of IoT- specific security threats will undoubtedly drive innovation in this space, enabling us to expect newer IoT- specific security technologies to appear in the creation phase in the near future. Many of these technologies may align around vertical and industry for specific use cases such as IoT in healthcare or IoT in industrial applications, etc. IoT security is integral to gain and retain consumer trust on privacy and fulfill the true potential of IoT, thus safeguard IoT for our secure future ■



Jayakrishnan shares the different security features which his organization takes to safeguard security of data assets

Security-In

Jayakrishnan P
Associate Vice President,
Muthoot Fincorp Ltd.

NEXT100 Winner 2016

At Muthoot Fincorp Limited, a RBI regulated NBFC with more than 3500 branches pan India, we look into security aspects with utmost importance. With increasing incidents of data breaches around the world, we are highly committed to safeguard the security of our data assets and interests of stakeholders.

We have implemented state-of-the-art data centers and disaster recovery centers with the most modern security features around the network. We have two layers of security around the network. The primary protection is by using firewalls at our datacenters. At the branch level we have the UTM Box and Symantec End-Point Protection solution enabled on all machines connected to the network. Using Symantec End Point Protection, we ensure that all the access to external devices are blocked. The UTM Box ensures that only whitelisted websites are accessed by users, thereby ensuring that there is no unauthorised access to other sites, and hence protecting us against malware or ransomware attacks.

I. Security Operations

a. Audit Logs and Events

The infrastructure team performs consistent monitoring of event

viewer and SEP logs for any unauthorized or suspicious access to the system and configuration files.

b. Network Access Control

Only authorized users and devices gain access to our networks. Any vulnerability is proactively identified and patched immediately. Wireless networks are managed by controllers with security policies and filters put in place with predefined protocols.

c. Network Protection and Standards

The enterprises' internal and external networks are protected from unauthorized activity. The network security team has implemented state-of-the-art network security and administration policies using Fortigate UTMs and Symantec Endpoint Protection Manager. Advisories from CERT-In are monitored by senior network specialists and all of them are implemented.

d. Mobile Security

All mobile devices are protected using Mobile Device Management (MDM). The MDM uses an enterprise-wide a product called Samsung Knox, which comes highly recommended. It was chosen after a thorough evaluation of competing products, and this was benchmarked as one of the most powerful products for MDM. Only application and settings defined in the MDM policies can be accessed in the device. All internal wireless access points are managed by Fortinet's product called FortiAP and configured with security policies and filters.

e. Protection against Malicious Code

We are protected against malicious code with SEP and FSRM on servers. The network devices are patched with the latest fixes as per vendor recommendations.

f. Background Checks on all Employees

Our Human Resource department performs background checks on all our employees including outsourced employees.

II. Threat & Vulnerability Management

a. Incident Management

Security incidents are managed with consistent and effective approach responding and recovering from a disruption. A proper identification of security events is performed using SEPM & Fortianalyzer reporting.

b. Patch Management

Patch management is performed using WSUS for Microsoft applications and Operating Systems.

c. Vendor Firmware Updates for Servers & Network Devices

Technical vulnerabilities are patched as per the advisories from vendors as well as CERT-In.

d. Application Vulnerability Assessment

All applications are VAPT tested and their vulnerability is addressed accordingly.

e. Security at Branch Level

All branches are equipped with CCTV and all motion based recording into the cloud for verification and alerts.

f. Emergency Response Team for Enhanced Security at Branches

An Emergency Response team has been constituted wherein a fleet of cars with security officers are alerted of any incidents at branches including attempt at breaking in, robbery, etc. and they make physical appearance at branches in their cluster. This provides an added layer of deterrence.

The Winning Tip

We have implemented **state-of-the-art datacenters and disaster recovery centers with the most modern security features** around the network

III. Identity Access Management

a. Access Control

Only authorized personnel are provided access to application systems, with appropriate levels of privilege. Frequent audits are conducted to weed out inactive users.

b. Maker Checker Rule

All our financial applications have maker checker facility as a security measure.

c. Authentication

At MFL, we have implemented a two level authentication using username and employee ID with strong passwords. External access is restricted, and is possible only through VPN client application. Emergency access is not given to unauthorized parties.

d. Operating System Security

System access is restricted with strong domain & local user credentials. All user accounts (mail, domain, VPN, application) are immediately disabled during NOC clearance.

e. Data Security

Data level security is implemented by using the hashing methodology whereby unwanted tampering of data is protected.

IV. Business Continuity Management

a. Disaster Recovery

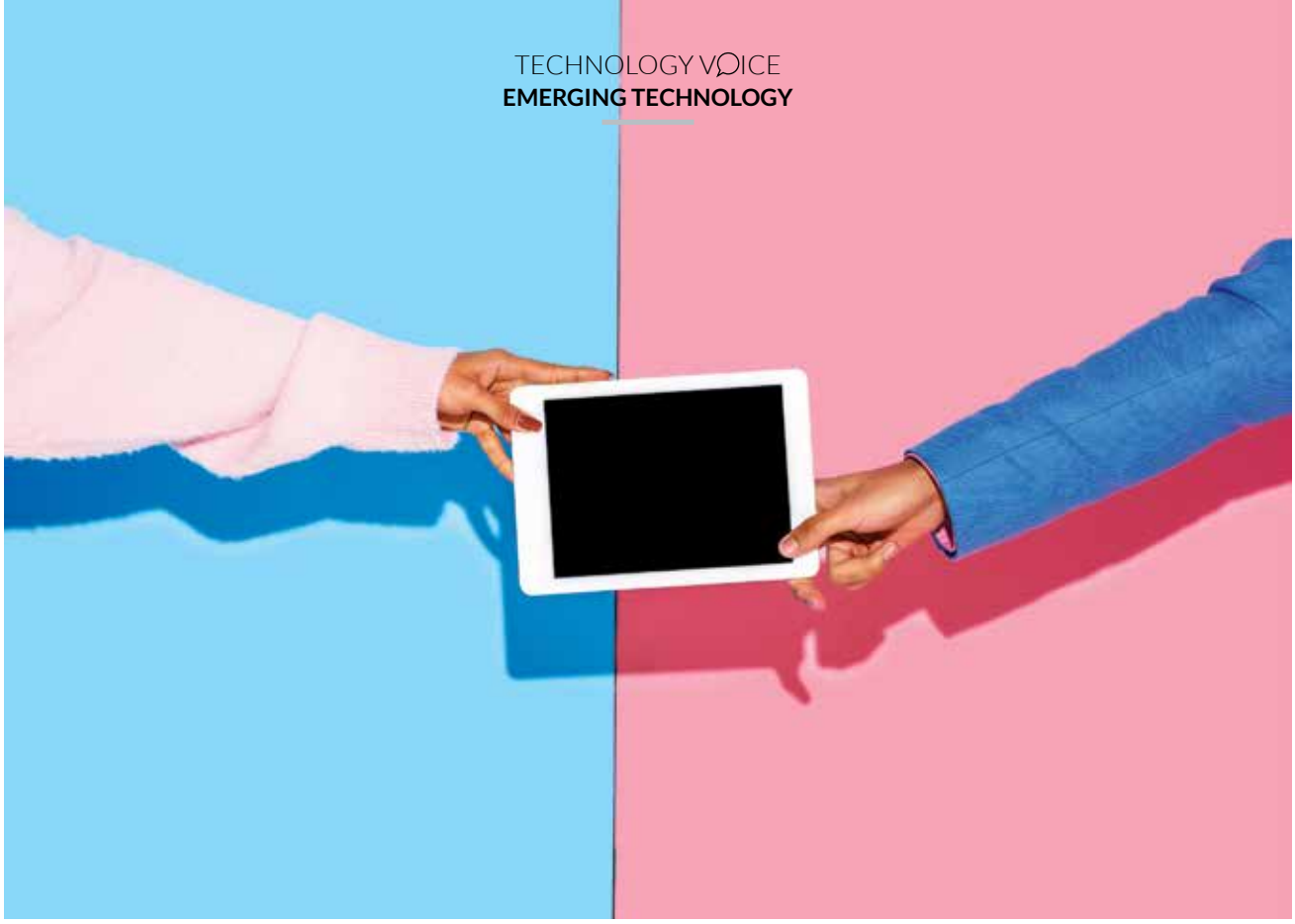
At MFL, we have implemented state-of-the-art data centers and disaster recovery centers with the most modern security features around the network. For Disaster Recovery (DR), we use Hyper-V replica and double-take as DR tools. DR Failover drills are carried out periodically.

b. Data Backup

We have defined backup and restore procedures. They are done using TSM and Symantec Backup Exec.

c. Physical Security

Our physical assets are in a protected environment. Our data center is a Tier-3 data center managed by SIFY at Electronic City, Bangalore. Only authorized personnel are provided access to the premises which are managed by SIFY security and their facilities management team. Being a Tier-3 Data center, it is also protected from environmental threats and hazards ■



Jegadeeswaran shares his perspective on the future applications of emerging technologies

Future Forward

Jegadeeswaran B
Assistant General Manager - IT, TVS Automobile Solutions Pvt. Ltd.

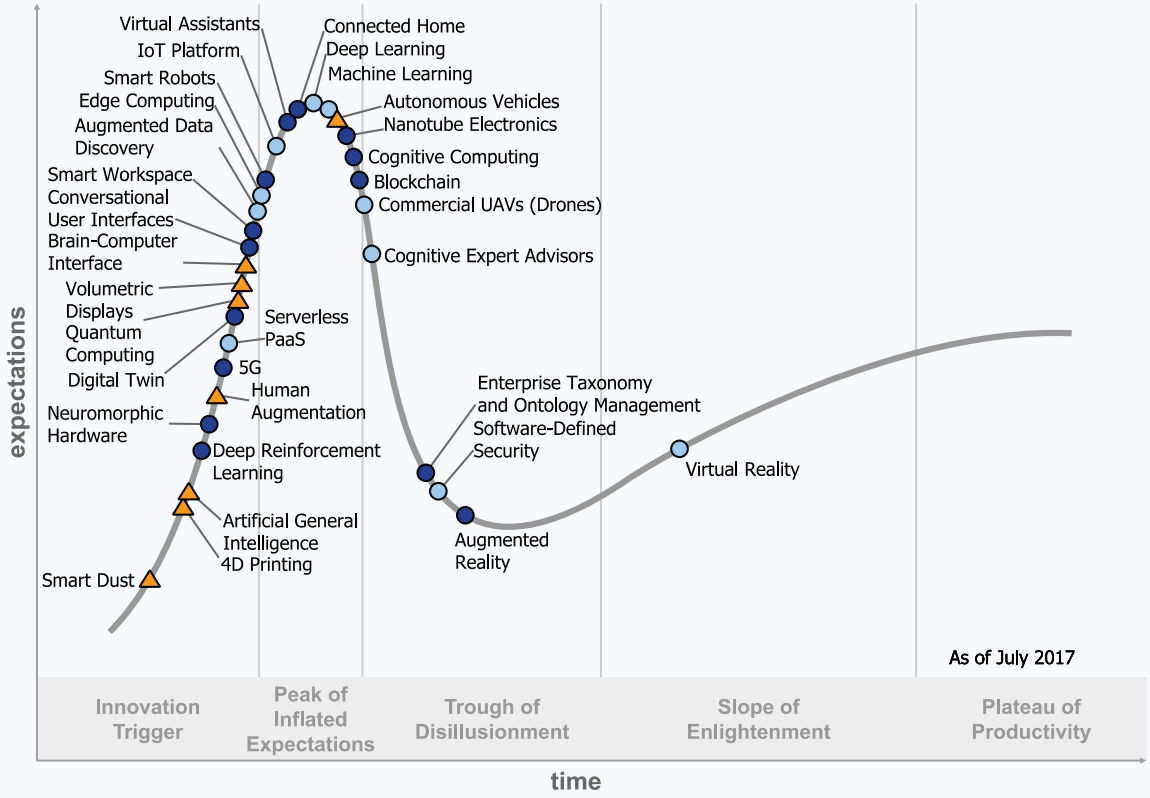
NEXT100 Winner 2017

We are living in a digital era and experts in their relevant domain are making tireless efforts to innovate new things successfully. One must agree that there are plenty of applications and technologies in use today. It is very difficult to discuss every one of them. However, I am presenting the top three technological trends along with necessary evidence:

"Organizations will continue to be faced with rapidly accelerating technology innovation that will profoundly impact the way they deal with their workforce, customers, and partners," says Mike J Walker, research director, Gartner. According to *Gartner's Hype Cycle for Emerging Technologies 2017*, there will be three distinct technologies namely AI everywhere, Transparently Immersive Experiences and Digital Platform, which intensely create new experiences with unrivalled intelligence, and offer platforms that propel organizations to connect with new business ecosystems in order to become competitive over the next five to ten years.

Gartner's *Hype Cycle* is a graphical depiction of a common pattern that arises with each new technological innovation. In Gartner's 2016 *Hype Cycle*, it was mentioned that three trends namely, blockchain, smart machines and IoT are emerging technologies. Here I would like to highlight the transformation of application of emerging technologies.

Hype Cycle for Emerging Technologies, 2017



Source: Gartner (July 2017)

Three Trends

AI Everywhere

Deep Learning
Deep Reinforcement Learning
Artificial General Intelligence
Autonomous Vehicles
Cognitive Computing
Commercial UAVs (Drones)
Conversational User Interfaces
Enterprise Taxonomy
Ontology Management
Machine Learning
Smart Dust
Smart Robots
Smart Workspace

Transparently Immersive Experiences

4D Printing
Augmented Reality
Brain-Computer Interface
Connected Home
Human Augmentation
Nanotube Electronis
Virtual Reality
Volumetric Displays

Digital Platforms

5G
Digital Twin
Edge Computing
Blockchain
IoT Platform
Neuromorphic Hardware
Quantum Computing
Serverless PaaS
Software-Defined Security

Source: Gartner 2017

Within a span of one year, *Hype Cycle for Emerging Technologies* has been evolving in parallel with consumer's consumption pattern, and that's why applications and technologies evolution is happening. Here, I am going to share more insights about application of emerging technologies 2017 by analyzing Gartner's report:

Digital Platform: Every organization obviously wants to do business through digital platform, and dedicated resources are made available to manage digital business as well.

Blockchain is one of the digital platforms that is more than just a buzzword. Blockchain technology is defined as a continuously growing list of records called blocks, which are linked and secured using cryptography. Blockchain has been a trend for some time now, and is gaining traction. It is expected to become mainstream in the next five to ten years.

In this highly competitive application technology arena, "Hashgraph" is now referred to as a superior application of emerging technology for the future. Swirlds is a software platform that has developed Hashgraph consensus algorithm, an entirely new distributed ledger technology that is much more cost-effective, believed to be 50,000 times faster (2,50,000 transactions per second), safer, more efficient and mathematically fairer than blockchain; however, no proof of work has yet being done to prove Hashgraph 's calibre. With this example, I believe I am able to correlate the context. Business and technology leaders are always looking forward to setup and make use of right technology for their business in the next five to ten years. The foremost challenge is technology becoming obsolete so quickly and thus, requiring enhancements to meet their stakeholder's expectations. To overcome these challenges, extremely flexible and scalable applications and technologies are preferred.

Choosing an appropriate digital platform with the above-mentioned qualities is exceedingly important. Every organization may take this as an opportunity rather than a challenge.

Transparently Immersive Experiences: Augmented Reality (AR) and Virtual Reality (VR) are other applications of emerging technologies, which are expected to upend the trend in the next five to ten years. AR is a live direct or indirect view of a physical environment whose elements are augmented by a computer generated sensory environment using sound, video, graphics and GPS. AR and VR are used in various sectors, such as education, manufacturing, healthcare, gaming, real estate and travel.

In India, governments of Kerala and Gujarat have already implemented AR in their respective tourism sectors. In education, AR and VR have made education more interactive; the learners can experience themselves through visual images and graphics for better learning. Google launched *Expeditions* in 2015, an AP and VR platform for classrooms. In the recent past, there are plenty of applications available for students. One example is the *Byjus* application, where they vouch 10 million students on the platform and 5 lakhs annual subscription. They are one of the very successful organizations in the last three years. The application is intuitive, illustrative, and visual objectives are attracting learners to understand the concepts of difficult problems in an easy way. AR and VR have revolutionized in healthcare industry as well. Accuvein, an AR handheld device scanner projects an image of the skin of the valves, veins and bifurcations underneath, which helps doctors and nurses to find out a vein while giving an injection.

Commercial UAVs (Drones): An Unmanned Aerial Vehicle (UAV), commonly called as Drone, is an aircraft without a pilot on board. A system of communications and a ground based controller are components of a drone. Drones are rapidly growing in popularity although they are still in the infancy stage in terms of adoption and usage. Primarily, government organizations are penetrating and making mass usage whereas certain industries are way behind, the reason being the absence of any guidelines. The amateur use of drones has so far been

The Winning Tip

AI everywhere, **transparently immersive experiences and digital platforms**, are the technological trends of the future

illegal in India. The Directorate General of Civil Aviation (DGCA), regulating agency for such vehicles (drones), unveiled a policy which will be in force very soon. The lightest category, Nano, a payload of up to 250 grams and flight to a maximum of 50 feet, warrants for one time registration. However, if the equipment which is more than 2kg, then the operator must get security clearance each time the drone is operated. But, the global trend is different from the Indian scenario. There are three big categories in drone technology: Military drone technology, Commercial drone technology and Personal drone technology.

According to report from Goldman Sachs, global militaries will spend USD 70 million on drones by 2020. Drone technology has seven potential generations and the majority of current technologies is in fifth and sixth generations. Generation 5 includes transformative designs, three-axis gimbals, 1080P HD video or higher value instrumentation and improved safety modes whereas Generation 6 includes commercial suitability, safety and regulatory based designs, platform and payload adaptability, automated safety modes, intelligent piloting models and full autonomy and air space awareness. However, research and development are in full swing to release Generation 7 which will include complete commercial suitability, fully compliant safety and regulatory standards-based design, platform and payload interchangeability, automated safety modes, enhanced intelligent piloting models and full autonomy, full airspace awareness and auto action (take off, landing, and mission execution) ■

Muneesh discusses the concept of DevOps in detail along with its benefits

Connecting DevOps

Muneesh Kumar
Vice President,
XcelServ Solutions

NEXT100 Winner 2017

DevOps, normally mistaken to be either a tool or a profile in an organization, is neither! It is a set of principles and practices that helps in continuous integration and development. DevOps is an application development method that stresses communication, collaboration and integration between the developers and Information Technology (IT) professionals. So, DevOps is a response to the interdependence of software development and IT operations that aims to help organizations to rapidly produce software products and services.

Given all its definitions and delusions, it is indeed more than interesting to note that if practiced correctly, the DevOps process has a few key practices that can help organizations to innovate faster through automating and streamlining the development and infrastructure management processes.

Now all the innovations in the process or the product are only possible if the methodologies are followed precisely, some of which are detailed below:

- One of the major and important practices is to perform very frequent updates. This help organizations to innovate faster for end customers. These small releases are usually more incremental,

make development less risky, and help the teams identify and address bugs quickly.

- Another way of making your application more robust and flexible is to use microservices. The combination of micro services and increased release frequency leads to significantly more deployments which can present operational challenges. DevOps practices such as continuous integration and continuous delivery solve these issues and let organizations deliver rapidly in a safe and reliable manner.
- Infrastructure automation practices such as, infrastructure as code and configuration management, help to keep computing resources elastic and responsive to frequent changes. In addition, the use of monitoring and logging helps engineers track the performance of applications and infrastructure, so they can quickly react to problems.
- Continuous Integration (CI) is nothing but software development practices that require the teams to merge their code into a central repository regularly, after each check-in automated build and test are run. But the goals of continuous integration are to find the defect quicker and improve the software quality, thus building more efficiency in the process.
- Continuous Delivery (CD) is a software engineering approach where the code is automatically built, test and released to the environment for testing or in production. This is a very important step in the development cycle as this entire hole cycle ensures the reliability of the software at any point.
- DevOps Culture is about removing the barriers between two traditionally siloed teams' development and operations and stresses on small, multidisciplinary teams, who work autonomously and yet take collective accountability for how actual users experience their software. For a DevOps team, there's no place like production. Everything they do is to improve customer experiences.
- Infrastructure as Code (IaC) helps to manage the development, production and testing in an efficient and repeatable manner through the management of virtual machines, networks, load balancers and connection topology in a descriptive model. The big advantage that IaC achieves this is by using the same versioning as the DevOps teams for source code.
- Infrastructure as Code has evolved, over a period, to solve the problem of environment drift in the release pipeline. Teams with integration of IaC in the process can deliver stable environments rapidly and at scale and can avoid manual configuration of environments with enforcement of consistency by representing the desired state of their environments.
- Microservices, especially the microservices architecture is a design approach to build a single application as a set of small services. The concept is to develop services like mini applications where each service runs in its own process and communicates with other services through a well-defined interface using a lightweight mechanism which is typically a HTTP-based application programming interface (API). This builds a huge capability in the system to develop, detect, manage a large product in small phases and yet maintain the impact on the system. Microservices are designed & built around business capabilities with each service scoped for one and only one purpose and deployed independently, either as a single service, or as a group of services.
- Monitoring, as it implies, provides feedback

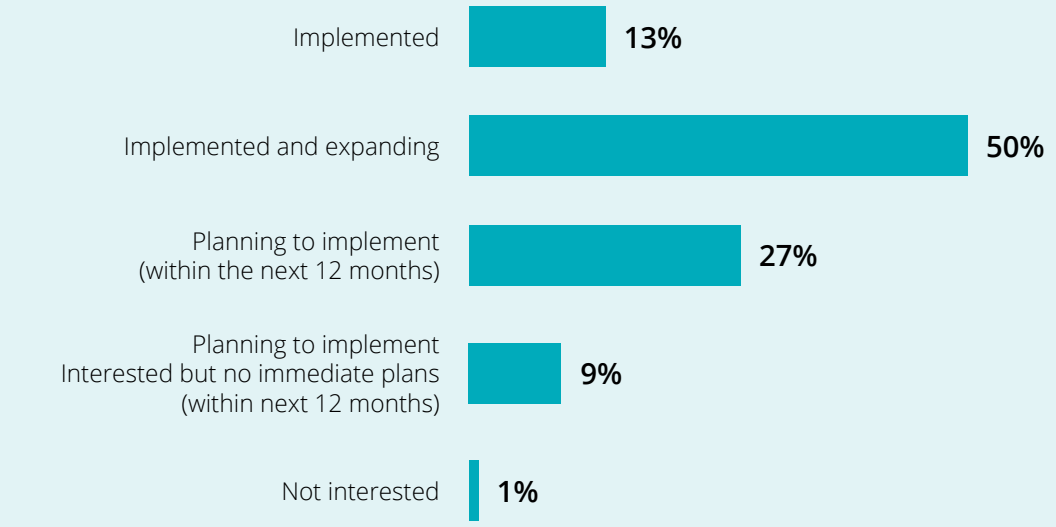
The Winning Tip

DevOps is a response to the **interdependence of software development and IT operations that aims to help an organization** to rapidly produce software products and services

DevOps Implementation

Six Trends That Will Shape DevOps Adoption In 2017 And Beyond

"Has your organization implemented DevOps? Where does it stand in relation to DevOps?"



Base: 237 DevOps pros

Source: Forrester's Q1 2017 Global DevOps Benchmark Online Survey

from production and is obviously the most important aspect of the DevOps process. One of the bigger goals of monitoring is to achieve higher availability by minimizing time to detect and mitigate along with building the capability of "validated learning" by tracking usage. Organizations can get to understand the most critical aspects of how the updates have impacted users and also shed more light on the root cause or all issues created through capturing, categorizing, analyzing data and logs generated by applications and infrastructure. As active monitoring becomes increasingly important - services must be available 24/7 and as application and infrastructure update frequency increases, creating and analyzing alerts and performing real-time analysis of this data will help organizations to act proactively. This segment delivers information about an application's performance and usage patterns.

- The DevOps toolchain is a combination of tools that enables DevOps lifecycle design, development and management of applications. These tools automate the manual tasks and help teams to manage the complex environments. Most of DevOps aspects won't be possible without tools such as, Jenkins, Ansible, Docker or Puppet. Still, tools such as, Team foundation Server and Teamcity only facilitate the process and allow to achieve the goal.

Some of the benefits of DevOps are as follows:

- Frequently and fast software delivery in the marketplace
- Minimizing the chance of outages; if anything goes wrong, the team can handle quickly
- Better collaborations between Business, Dev and Ops teams
- Stabile environments
- Less complexity to manage
- Time to focus and quality improvement

The purpose of DevOps is not to create silos but to create a strategy for better collaboration between various cross-functional teams. The implementation of DevOps in early stages creates a foundation for scalable growth. So, DevOps is not a team but a concept; however, if you still want to label a team as DevOps, think again! ■

Rupen discusses the potential IT security threats and the measures taken to prevent them

Hack-a-ton

Rupen Shah
Assistant General Manager - IT, Arohan Financial Services Pvt. Ltd.

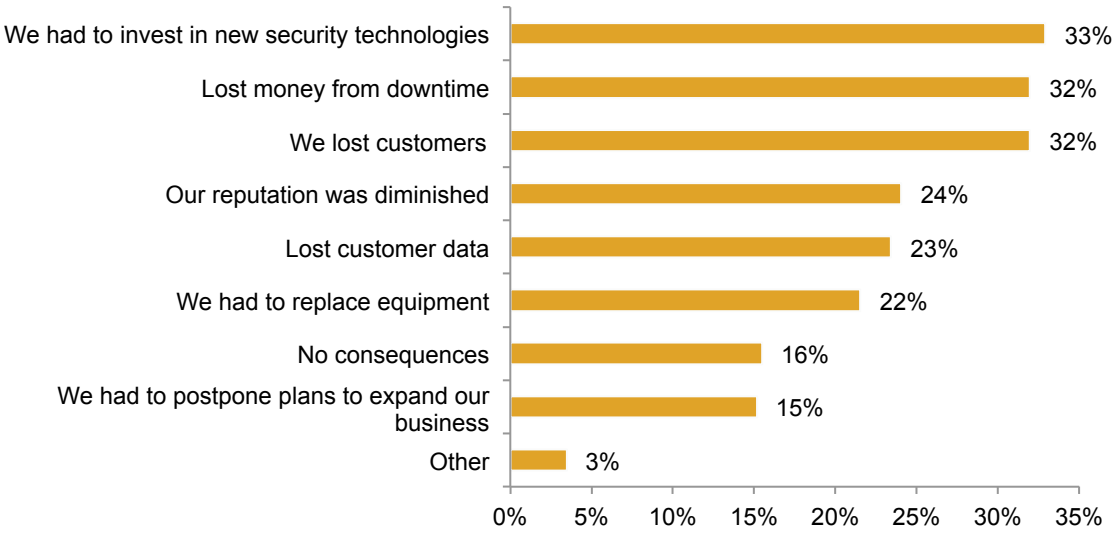
NEXT100 Winner 2017

'IT Security' and Internet of Things (IoT) are of great significance in today's digitally connected world. The rapid pace of getting everything connected and online in a "smart" world is creating new vulnerabilities that can be exploited by hackers.

Ransomware as a concept around for years now but has recently evolved. Hacking group, "The Shadow Brokers", was behind the WannaCry Ransomware outbreak which used unpatched OS level vulnerabilities originally discovered by another "grey" group, "The Equation Group", which according to speculation is associated with the US National Security Agency.

It is speculated that the NSA-backed "Shadow Brokers" actually pays software conglomerates to NOT patch the vulnerabilities discovered in their software until they are revealed publicly. This is to allow US agencies in their clandestine espionage activities against other countries using the software. It is a well-known fact that Microsoft patched the SMB vulnerability in March 2017 only when the exploit was already published in February, on the Dark Web and Internet.

What were the consequences of the ransomware attack?



Source: Ponemon Institute Research Report

Ransomware attacks were predicted to cost an aggregate of USD 5 billion in 2017 alone. Soon after WannaCry in June 2017, another Ransomware Petya crippled Fortune 500 Shipping company, Maersk Lines, when their systems were affected for days leading to estimated losses of USD 300 million.

With the governments push for creating a cashless economy by empowering all users with digital apps, Aadhaar linking with bank accounts, OTP-based two-facto authentication, we are also creating new vulnerabilities for exploitation by hackers.

Consider the scenario where a of ransomware encrypts our data and demands a ransom for decryption keys. Such malicious software can sneak into our smartphones in the guise of an app and get permission to access messages and reply to the messages in an automated fashion.

Even today, there are "applications" that are designed to "read" and capture "OTPs" sent by banks and submit to e-commerce sites for validating our online transactions; the only user interaction required is a click on the "Submit" button. Some users inadvertently save their credit/debit card data on their phones memory for auto-populating the various fields in the online transaction screen. This leaves the user exposed to such malicious e-robbers who can wipe out your bank accounts after reading, misusing and deleting the OTP message stealthily.

User awareness is the key to protect against such e-robbery, such as, using virtual credit card numbers with fixed denomination approved namely, Net-safe which is provided by HDFC Bank etc.. These one-time use CC/DC numbers cannot be misused even if known to someone after the first-use.

The recent steps by RBI to make it mandatory for banks and NBFCs to report security breaches is a welcome step which puts the banks' processes under scanner and will force them to revisit, re-analyze, and strengthen their online financial processes ■

The Winning Tip

With the govt's push for creating a cashless economy by empowering all users with **digital apps, Aadhaar linking with Bank accounts,** we are creating new vulnerabilities for exploitation by hackers

Sasikumar shares his views on the challenges, laws, standards and certifications related to IT security

Future Secure

The first step in improving the security of IT system is to answer these basic questions:

- What am I trying to protect and how much is it worth to me?
- What do I need to protect against?
- How much time, effort, and money am I willing to expend to obtain adequate protection?

These questions form the basis of the process known as risk assessment. Risk assessment is a very important part of the IT security process. We cannot formulate protections if we do not know what we are protecting those things against. After we know our risks, we can plan the policies and techniques that we need to implement to reduce those risks.

IT security plays a prime role in helping create the environment needed to set the ground for implementing successful Information Technology (IT) plans. IT security is a complex topic and evolves almost as fast as technology does.

If we use computers at home or at work, we have a certain level of responsibility. Security is everyone's responsibility, whether you are a regular or non-regular user, server administrator, network administrator, manager or a general manager; with responsibility

SN Sasikumar
Assistant General Manager,
TVS & Sons Pvt. Ltd.

NEXT100 Winner 2017

for systems or networks, understanding what the central security issues are, taking prudent actions to protect our systems, and putting a set of effective security policies in place.

These are critical steps we must take to ensure that our IT systems and information will be secure from unauthorized access and that will be able to exchange that information securely with others on the network.

Many technically skilled people use computers; so advice and assistance from peers is easily obtained. When computer or network problems arise, such as the spread of a virus, there is a rich set of information channels through which news and security patches are transmitted.

Failures in security occur in organizations and few breaches are made public in the press or known through various electronic social media (Facebook, Twitter, etc.). Many failures are not reported as leakage of IT security breaches in public knowledge could lead to further intrusions and unwanted results. Organizations can generally withstand some level of security failure. However, the consequences of security failures in occurrence could be considerably more serious, because lack of awareness may lead to more massive breaches, and a malicious attack may be more disastrous, in terms of money, reputational effects and loss of trust.

A criminal activity will migrate to places where controls are poor and security is weak. The IT system activities are likely to make interesting targets in companies that are less conscious of IT security. Organizations need to build capacity in terms of trained human resources and in terms of the technological infrastructure that will protect them from being easy targets of hackers.

With the emergence of voice over IP, digital telephony protocols that are increasingly used, and the emergence of 4G in India and 5G technologies in the US and other developed nations, security issues in this space need to be clearly understood and addressed.

Emerging Technology Adoption Threats Create Complexity

The IT environment is changing rapidly with the introduction of new products, especially digital revolution of mobile devices, laptops, cellular phones, which present different challenges to infrastructure and data security. Emerging computing applications including e-commerce also create complexity in the networked environment. From ATM machines to online banking, these capabilities offer convenience and cost savings, but they also introduce new opportunities for theft and fraud. To make matters worse, would-be attackers are now able to develop blended threats, combinations of Trojans viruses, and worms that may cause greater damage to IT systems and data than the individual forms of such "malware". Since these developments affect users of technology in the organization, awareness of general IT security issues, including the existence and prevalence of specific security threats will help users, managers, and policy makers design effective strategies to strengthen their networks, at home and at work, against breaches.

The Winning Tip

IT security plays a prime role in helping **create the environment needed to set the ground for implementing** successful Information Technology plans

IT Management

In spite of the challenges, IT managers in the public and private companies are investing in new tools and communication technologies (like e-mail, VOIP and Wi-Fi) and business software to assist in running their day-to-day operations. The advantages in efficiency, outreach, and cost savings in these IT devices and services are clear:

- E-mail improves business communications with customers, partners and suppliers
- VOIP provides an expanded data protection and management capabilities, resulting in better record-keeping for financial managers, better customer analysis for sales and marketing managers, and better production statistics for line managers
- Wi-Fi enhances the ability to access large quan-

tities of information quickly and cheaply

However, these improvements are not without risk, and thus, some organizations may choose to outsource their security needs. Some experts say that outsourcing for non-core services like IT security has been the corporate strategy. In addition, some organizations have a specific interest in global security needs, particularly those of developing countries. As an example, the Information System Audit and Control Association (ISACA) has partnerships in all major countries and provides cases from various countries, and programs, all available as open source. ISACA also offers an audit and control framework for organizations and includes checklists for outsourcing situations. Whether conducted and controlled in-house or through outside vendors, developing and maintaining strong security infrastructure, policies, and procedures is a balancing act for most enterprises. Executives, managers, and policymakers must weigh the risks and set a standard that balances the investment in security with the official objectives and bottom line growth of the company. Once a company has achieved the desired level of security, the management must not forget the importance of maintaining up-to-date systems and performing regular audits of the security plan. Security is an art form, rather than a science, and requires the coordination of many creative thinkers to ensure its successful impact on an organization and society as a whole.

Digital Transformation

Regulators should consider how broadly to extend supervision and enforcement over transmission method. The primary reason by most people for refusing to use electronic transmission method is fear that the information is not adequately protected. However, now people have started understanding and adopting the electronic transmission mode of payment in their day-to-day life (Digital wallets such as, Paytm, OLA Money, PhonePe, etc.) and the drive of digital transformation from the present Narendra Modi government. Proper protection could strengthen consumer confidence and market discipline, paving the way for greater use of electronic financial systems.

IT Security Laws

All the countries now put in place IT laws addressing abuses of a computer or network that result in loss or destruction to the computer or network, as well as associated losses. The law should also provide the tools and resources needed to investigate, prosecute, and punish perpetrators of cyber crimes.

One key issue realized most of the companies or countries' need to improve information exchange between regulatory and law enforcement agencies. Many companies/countries have several agencies for gathering critical information.The data is shared by these agencies or with the agencies of other nations (sometimes for legal reasons), as governments try to leverage scarce resources in order to regulate and battle crime in the electronic environment; thus, making information sharing and international cooperation a critical activity.

Standards, Roles and Certification

Both public and private entities should work cooperatively to develop standards and harmonize certification schemes. The two categories that require particular attention in terms of certification are electronic security service providers and transaction elements. In order to enable secure electronic transaction, financial regulators would require licensing of vendors that directly affect the payment system. The security industry has developed a Security Expert certification. By using a certification approach, the industry benefits by providing consumers with a recognizable structure, accountability between the industry and its experts, and a means of separating the approved expert from the self-proclaimed expert. It also elevates the field of security to a professional status and creates an incentive for the industry to raise and protect standards ■

Sandeep proposes an Application Classification Framework, which aims to standardize and industrialize Infrastructure Support (IS) services

Apping IT

Sandeep Gupta
Manager,
A.T. Kearney Limited,
UK

NEXT100 Winner 2011

Enterprise IT managers have actively been moving to outcomes based commercial constructs such as Managed Services for operational functions such as, Application Maintenance and Support. This model has been successfully industrialized for Infrastructure Support (IS) services, wherein the entire IS service work gets efficiently decomposed into well-defined Resource- Unit (RU) which can benchmarked, priced, bundled and governed by outcome-based SLAs. Application Maintenance and Support (AMS) has lagged in its industrialization journey partly due to lack of consensus on how to decompose various services into units of work.

AMS Managed Services deals are usually based on fixed prices for application bundles or projected ticked volume or a combination of the two. These deals leave most of the control and visibility of efficiencies in the hands of the vendors who are often the primary beneficiaries of the said efficiencies. Some leading organizations have started experimenting with AMS deals based on per application pricing driven from a classification framework covering variables, such as workload, criticality, etc. These

frameworks not only create a unit-driven pricing mechanism for AMS but also facilitate proactive application portfolio management. The lynchpin of this approach is a robust application classification framework, often the least understood aspect of managed services model due to the variety of frameworks being used by vendors, often to their own advantage.

Many organizations are frustrated by the 'Black-Box' nature of many Managed Services deals and seek to gain a better understanding of the services they receive and the levers employed to deliver efficiencies. Our framework attempts to provide the necessary transparency while staying true to the spirit of supplier owned managed services delivery model.

Application Classification Framework

Our experience indicates that a move to a standard application classification framework can yield several benefits:

- Consistent and objective definition of effort needed for application support, as it is driven off operational data
- Allows for easy change management in case of Adds and Deletes in the portfolio
- Facilitates a structured approach to driving efficiency in the portfolio where the vendor must demonstrate increasing application stability and reducing workload
- Minimizes wild swings in workload estimates as it is not driven by ticket volume only

An adequate model must reflect the complexity of the application landscape while not creating a large administrative burden. It is also critical to define the model prior to engaging with any service providers. The key principles of a classification framework include:

1. Objectively and transparency – be data driven (ticketed and non-ticketed workload, business impact, etc.)

2. Technology requirements and support risk profiling

3. An ability to predict support cost for new applications

We propose a four-stage approach for developing an Application Classification Framework (see Figure 1). The framework enables a structured Change Management process that allows additions and deletion of applications from the portfolio.

1. Application Profiling: The process starts with creating profiles for applications in the inventory based on set criteria that includes Activity/ Workload, Technical Complexity and Support Criticality. Each profiling criteria comprises numerous sub-parameters to ensure each application is profiled to an adequately granular level. The next step is to gather historical data for each of the sub-parameters. The time-period for which the historical data is gathered for profiling is critical to ensure that seasonal spikes in support activity (at quarter or year end, for example, or during peri-

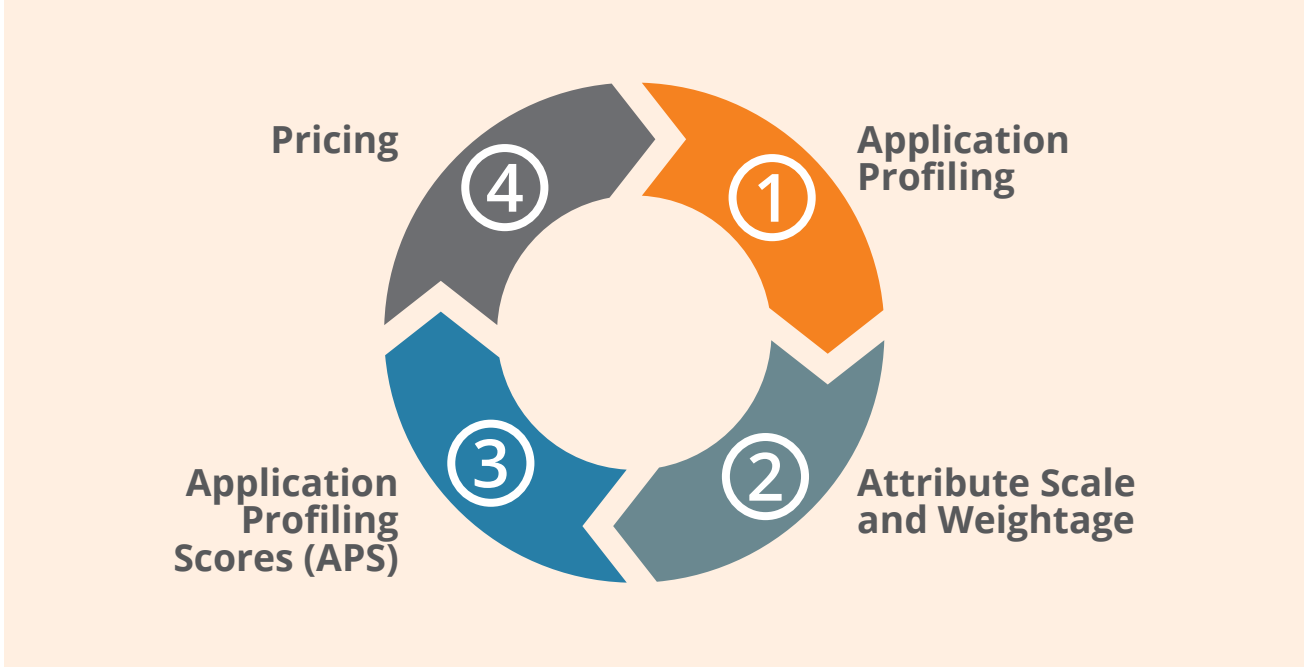


Figure 1

Profiling Criteria	Sample Sub-Parameters	Description
Activity / Workload	Number of Incidents, Service Requests, Problems, Known Errors	Profiles the application based on the number of tickets and type of issues
Technical Complexity	Number of Critical Interfaces, Screens, Batch Jobs, Technology Score	Profiles the application based on technical complexity to support the application
Support Criticality	Number of Active End-users, Coverage Hours, Business Criticality	Profiles the application based on end-usage and business criticality.

Table 1

Major Category	Parameter	Weightage (a)	Score (b)	Category Score Σ (axb)
Activity/ Workload	Incidents	35%	3	3.4
	Service Requests	25%	2	
	Number of Problems	20%	4	
	Number of Known Errors	20%	3	
Technical Complexity	Number of Critical Application Interfaces	25%	1	1
	Application Technology Score	25%	1	
	Number of Batch Jobs	25%	0	
	Number of Screens	25%	1	
Support Criticality	Number of Active End-users	25%	0.8	0.8
	Support Coverage Required	25%	0.8	
	Functional Criticality	50%	0.8	
		Total App Score		**55.2**
		App Category		**A**

Table 2

ods of very high usage), get adequately covered.

2. Attribute Weights and Scoring: Once historical data has been gathered for the sub-parameters under each of the profiling criteria, the IT and business needs to collaboratively assign weights and scores for each sub-parameter.

Weights are applied to each of the sub-parameters, an example of which is shown in Table 2. Weights should reflect the organization's relative tolerance towards specific sub-parameters.

The sub-parameters are then **Scored** on a 5-point Likert scale. The data collected for each sub-parameter in step 1 need to be normalized on 5-point scale. *(see Table 3 for sample scale definition for Number of incidents sub-parameter)*

3. Application Profiling Scores (APS): Application profile score is computed as an

Minimum	Maximum	Scale
0	10	1
11	20	2
21	50	3
51	100	4
101	>101	5

Table 3: Scale for Number of Incident Sub-parameter

Application Profile Score	Application Class
>12.5	Class A
>10.0 and <= 12.5	Class B
>7.5 and <= 10.0	Class C
>5.0 and <= 7.5	Class D
<= 5.0	Class E

Table 4

The Winning Tip

A structured AMS framework aligns **the incentives for the buyers and suppliers** while providing transparency to all parties

aggregation of attribute scores and weights. The applications are then classified into bands, based on these scores. (see Table 4)

The sample structure shows 'A' class applications are of the highest importance to the business and hence will need to have the strongest SLAs, penalties, and monitoring.

4. Pricing Bands based on Application Classes: Post classification, the pricing bands get defined for each Application Class. The price band needs to be defined in consultation with the vendor – the highest scoring class commands the highest price per application regardless of the functional area it supports. Lower classes reflect lower workload and hence lower prices.

At the end of each billing period, the supplier bills the client based on the number of apps in each Class through a "Price-X-Quantity" exercise. This process also facilities change management as new applications added to the portfolio are added to the quantities based on tehri class and the ones removed are likewise taken out of the count.

Impact on Application Portfolio Management

The application classification framework is not merely a tool to manage contracts with vendors; it is in fact a key component of the application portfolio management framework. For it to have the maximum impact, the application classes must be tied to an application rationalization efforts or the typical 'Invest', 'Migrate' and 'Eliminate' framework.

Vendors should be required to shift apps from the higher classes to lower ones through reduction in workload by automation, shift left or other efforts leading to improved portfolio stability.

To summarise, large AMS organizations can receive a one-time transactional savings from signing a Managed Services deal, however, sustained year-over-year improvements are likely to remain elusive in the absence of a structured AMS framework – one that aligns the incentives for the buyers and suppliers while providing transparency to all parties. The proposed framework helps standardize and industrialize a service that has hitherto been challenging to manage for many organizations ■

Vikas envisions a world beyond mobility, envisioning the world of ubiquitous computing, which is both intelligent and pervasive

Goodbye, Mobility!

Vikas Gupta
Head-IT,
Essar India

NEXT100 Winner 2016

We are in the most interesting times today...the times of "Tsunami Transformation". In such an evolutionary stage of transformation, it is sometimes very difficult to pin-point the stage of transformation that we are in.

If we take a look at the history of interaction, you will realize that every form of human interaction is unique to the actors involved; heterogeneity is what defines us as humans.

Just visualize how interactions have transformed over times.

Circa 1440 BC, Moses receives the 10 commandments on the two not-so-lightweight Blue Sapphire stone tablets called Tablets of Testimony. Fast forward to the early 19th century when the first typewriter was developed comprising 2500 parts, and enter developments in mid 50s of the erstwhile century when the foundations of avatar of the current IT were laid.

As technology has progressed, these tools have evolved into standalone devices that could support more forms of interaction—hence the emergence of the mobile smartphone, a small computer that allows us to stay connected and helps us interact with people and computers in a variety of ways.

The locus of innovation has moved to the world of the con-

sumer, which had previously been, firmly, in the realm of business technology. The opportunity to use consumer devices and other on-demand services for business purposes has given rise to a concept called consumerization of IT.

Welcome to the world of Mobility!

Here you are served everything from snack-on-the-go to formally closing a multi-billion dollar deal; collaborated invisibly and virtually.

The customers' expectations of total mobility, ever-faster connectivity, personalized services and perfect instantaneous delivery seem to be growing as quickly as their data usage. At the same time, the pace of change is unprecedented – cloud, M2M communications, rapidly evolving world of devices and apps, etc.

Expectations and technology are feeding into each other, creating the need for faster innovation and time to market, improved network infrastructure, and so on.

Impact

For most part, hardware peripherals will probably not see a substantial impact from mobility. The area most impacted by mobility is the network and the impact is both:

- Constructive —creation of newer network infrastructures—and
- Destructive —obsolescence of older technologies.

Newer and faster network standards are excellent from point of view of very high throughput using Multiple Input Multiple Output (MIMO) systems, in the range of over 100 Mbps.

When it comes to IT facilities, Mobility will change the way employees operate. Workplaces will actually shrink to the size of a small mobile device while coverage of work itself, and go beyond the confines of physical establishments.

Below are some examples of umpteen possibilities in the future:

Bluetooth-enabled mobile devices carried by fire marshals in factory premises, keep updating their current position on the floor supervisor's dashboard through wall-mounted sensors, resulting in faster response time.

Richness in communication channels will help product development and marketing, where enterprises can exploit augmented reality applications for product demonstrations, and to address consumer pain points faster and more effectively.

Applications already allow smartphones to scan **barcodes**. Coupled with this, RFID tags connected to inventory items can be read using Near Field Communication (NFC) enabled mobile devices and supply chain managers will get real-time information on materials movement in ERPs, crucial in a Just-In-Time (JIT) environment, reducing inventory costs to a bare minimum.

Same RFID tags will also help with quality control.

Surveillance of plant facilities or premises under large uneven topography are being aided by enterprise mobility without the need for expensive wiring.

Sensors on machines in a factory allow technicians to know when maintenance is needed.

Mobility will develop wireless M2M and human-machine-interfaces, allowing designated personnel to supervise and control shop-floor activities from anywhere, demonstrating ubiquitous control.

With all this happening in the mobility space

The Winning Tip

While current mobility patterns are based on **menu-driven and GUI-based tools, ubiquitous computing holds the promise of understanding natural human interactions** such as presence, movement, or speech

at a lightening pace, this mobility trend, which still is in infancy, is auto-terminating into something called Ubiquitous Computing, which is both intelligent and pervasive.

Below are key differences between mobility and ubiquitous computing:

Ubiquitous computing lets the environment connect to you in many unobtrusive ways whereas Mobility took computers from desktop and put them in your pocket.

Ubiquitous computing sends information seamlessly into your environment, where numerous tiny devices monitor you, connect with you, and even think for you.

While current mobility patterns are based on menu-driven and GUI-based tools, ubiquitous computing holds the promise of understanding natural human interactions such as presence, movement, or speech.

A lot of ubiquitous computing is already in use.

Today when I enter my office, the lights come on automatically and when I leave, they go off.

In the near future, several actions may be triggered as I set out to work. For instance, smart cars will suggest an optimal route by assessing traffic along a smart city network. My virtual assistant may send an alert and the office temperature will adjust to my preference. My desk will show high priority tasks and the scheduler will prepare visitor passes for guests. The cafeteria will receive a request for preferred beverages. We may be able to automatically connect to video conference on the basis of confirmed invitations. The translation services based on the geography of our customers will be activated.

In short, when many smart devices connect, an intelligent environment will get created – envisioning a world of ubiquitous computing.

So long, Mobility! ■

Closing Note

I would like to thank all the NEXT100 contributors who took the time out of their busy schedules to share their thoughts and experiences on technology. As Benjamin Franklin, one of the Founding Fathers of the United States, once said, "To not be forgotten (sic) either write things worth reading, or do things worth the writing."

Why do I quote Franklin?

In his lifetime, Franklin was a lot of things. He was a renowned polymath, printer, political theorist, politician, freemason, postmaster, humorist, civic activist, statesman, and diplomat. Among all these titles, he was also an author who helped draft the Declaration of Independence and the U.S. Constitution.

He was also a scientist whose pursuits included investigations into electricity, mathematics and mapmaking.

Today's IT managers also need to wear multiple hats - those of leaders, techies and business strategists. We are super excited that we have played a small role in unleashing yet another aspect of their multifaceted talent - writing.

I will also like to thank those who have shared their technology pieces with us (those will appear in the January 2018 issue) and would like to encourage others who have queried but are yet to send their articles.

I must also mention that you do not have to be a NEXT100 winner to write for us. We would like senior IT managers to contribute for us all the time and not wait for a special issue.

We hope that you enjoy reading this! Suggestions and feedback are more than welcome, as always.

Thank you,
Shubhra Rishi
Associate Editor
IT Next


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


OYO
OYO has more than doubled business leads
Vodafone's Digital Engagement Platform
OYO was able to identify and communicate with customers effectively, improving lead generation by 250% and creating long-term revenue growth.
WIRE | WIRELESS | CLOUD | IOT
vodafone.in/business
1800 123 123 123
O&M 32
The future is exciting.
Ready?
vodafone