Opinion: | Pg 14
Securing The Digital Supply Chain

Insight: | Pg 30
Why Cryptocurrency Security Should Be On Everyone's Radar?

ITNEXT
FOR THE NEXT GENERATION OF CIOs

LEADING DIGITAL

How can enterprise IT managers make good digital leaders?

Why 2018 will be a tipping point for women in enterprise IT

PLUS: an analysis of the Indian CDOscape

April 2018 | ₹100 | Volume 08 | Issue 12 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

10TH ANNUAL
CSO SUMMIT

WHAT'S NEXT?

nextCSO & AWARDS

THE SEARCH FOR INDIA's FUTURE CSOs

25th-26th May 2018 | Crowne Plaza, Greater Noida, UP

79% of organisations identify cyber security as a top five business risk.

58% include cyber risk in their boardroom agenda.

51% have increased their cyber security budget.

29% believe their cyber security teams need major skills and talent enhancement.

25th - 26th May 2018

Crowne Plaza, Greater Noida

ARE YOU THERE?

Source -https://goo.gl/JDq3hn

Presenting Partner: Google Cloud

Associate Partner: eScan Enterprise Security

Organised by: CSOFORUM

A Brand of: 9.9 GROUP

CDOs Are From Mars...

Four nine or five nine is the holy grail of CIOs while the transformation heads talk of failure in the same breath as the initiatives—with a smile!

Shyamanuja Das

This issue's cover story is mostly (not fully) based on my research on digital transformation journey in selected companies within some of the largest groups in India—Tata, Mahindra & Mahindra and Vedanta/Sterlite.

When I spoke with people leading transformation as well as with some other CXOs, I realized what they talked about digital transformation and what I had heard till then, largely from CIOs were two completely different things.

While most CIOs talk about the need to understand business, most CDOs and transformation heads talk about culture and change management. While CIOs give examples of projects, the transformation head illustrate their points with examples related to training, reorganization and process transformation.

Continuously scanning tech landscape to identify new technologies that have the potential to create value for the business figures as one of the most important tasks in the digital journey, in the discourse among the CDO community. In the enterprise IT circle, such managers are poohpoohed as those lacking 'in-depth' knowledge.

Four nine or five nine is the holy grail of CIOs while the transformation heads talk of failure in the same breath as the initiatives—with a smile!

And both the communities are talking sense: as far as their jobs go. A CIO has to ensure that business as usual does not get impacted even slightly. If it does, a company may lose millions in a matter of minutes. A CDO has the mandate to disrupt. By definition, his successful project will cannibalize the existing business.

So, no one is right or wrong. But if you want to lead digital transformation, you have to get out of the CIO mindset. You cannot run transformation with your CIO mindset the same way a disruptor in charge of a mission-critical data center may become a disaster.

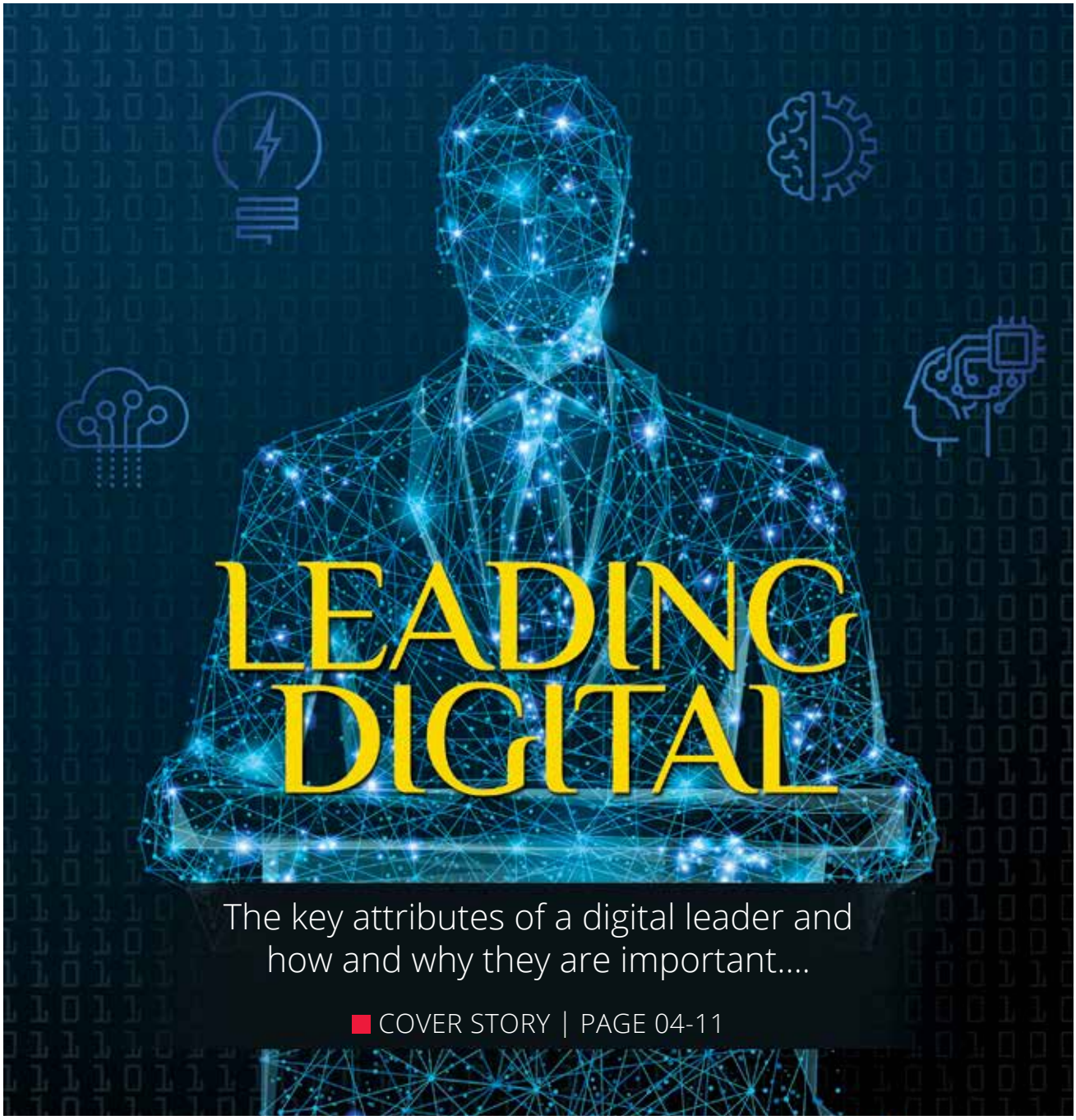
Good thing is, unlike some of the impatient marketing guys of yesteryears, most of the people driving transformation have a healthy respect for the enterprise IT guys. They do understand that without enterprise IT running the business well, they cannot afford to do the experiments. They also realize that many of the execution will require the expertise and skills of CIO and his team.

So, the importance of enterprise IT is not diminished at all. However, if you want to get into driving digital, you need to change.

How? Well, read the story.

APRIL 2018
VOLUME 08 | ISSUE 12

Content



The key attributes of a digital leader and how and why they are important....

COVER STORY | PAGE 04-11

COVER Design:
MANOJ KUMAR VP

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

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

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

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

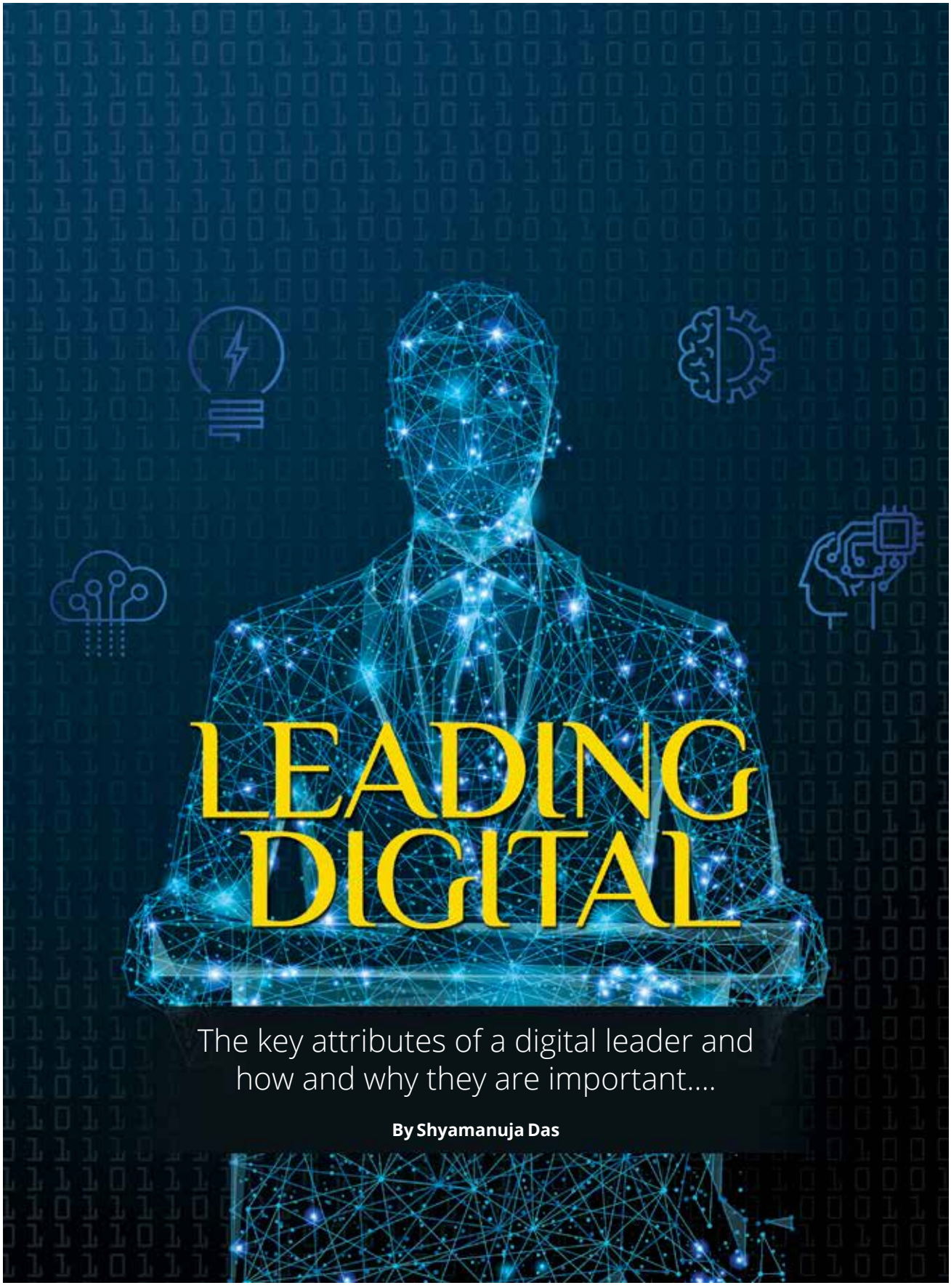
Manager - Events: Naveen Kumar
Manager - Events: Himanshu Kumar

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

OFFICE ADDRESS
9.9 Group Pvt. Ltd.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.)
121- Patparganj, Mayur Vihar, Phase - I
Near Mandir Masjid, Delhi-110091

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

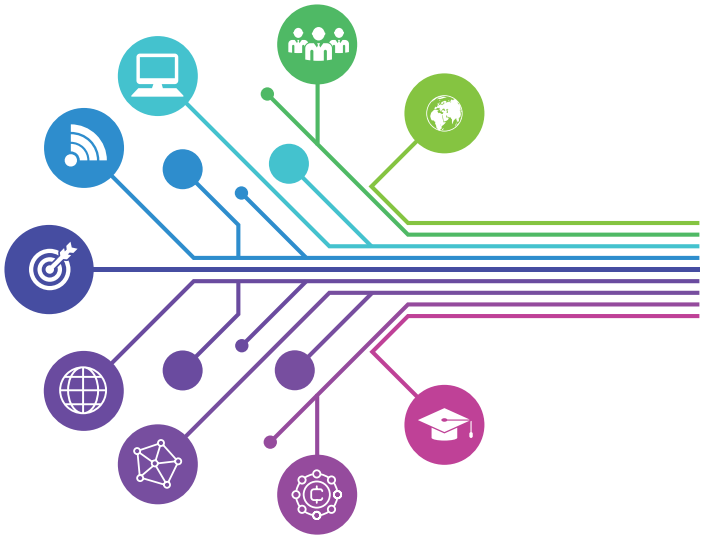
Editor: Vikas Gupta



LEADING DIGITAL

The key attributes of a digital leader and how and why they are important....

By Shyamanuja Das



By this time, you are probably more than convinced that digital is not another flavor of the season. It is here to stay and it is changing the business for real.

But have you felt that while your organization is going all out for digital, there is something missing for you? You are involved, but not quite in charge.

Your apprehensions are not quite baseless.

By the end of 2017, Corporate India had 44 designated Chief Digital Officers/Chief Transformations Officers, not counting those in ad/marketing agencies. Only 13 out of them are with a tech background. That is less than one-third. And just three of them handled both CIO and CDO roles. That is less than one out of ten.

Is the digital revolution just passing Enterprise IT? Is technology today too important to be left to technologists?

Not quite. At least not yet. But such an eventuality is not entirely implausible. Bad news is: Your worst fear may come true. Good news is: You can take the issue head-on.

Many digitals; many digitalists

To answer this question, we need to step back a bit and try to understand what exactly do organizations mean when they say digital journey?

"Transformation is a customized recipe for each organization," says Nischal Gupta, Chief Transformation Officer of Sterlite Technologies, a Vedanta Group-promoted, public listed company that is transforming from a cable manufacturer to a telecom solutions company.

Naturally, the role that each of the components play in the transformation—technology included—would vary from company to company, which, in turn may influence how they look at the role of enterprise IT too.

But a bigger factor is the 'multiplicity' or 'vagueness'—depending on which side of the debate you

The story is largely based on a research that we did on digital transformation journeys in some of the large groups in India. A story based on the research, *Decoding Digital Transformation*, appeared in the March issue of CIO&Leader that looks at the issue from the organization's point of view. Some supplementary research was conducted for this story.

are in—of the word 'digital". Organizations may refer to very different things when they say 'digital' or 'digital transformation'.

"Not many companies come to us saying they need to hire a digital transformation head. People are more precise about what they want," says Maneesh Dube, consultant and Head of India Ops at top executive search firm Russell Reynolds.

He puts the digital journeys into roughly three baskets.

First is the quick-impact changes around front-end customer facing activities. This is often to show that you are keeping with the times, in the eyes of the customer. Typically initiated by B2C companies, the journey is marked largely by better use of digital media leading to better customer experience and often, efficiency gains. The change at front-end, though it does impact some of the backend processes, does not necessarily need the entire organization to change.

"This is not really transformation but very much a full-fledged digital journey. The kind of people who are expected to lead this journey are those who understand consumers well, like marketing people," says Dube. Examples include Uma Talreja, CDO at Raymonds, Ajay Kaul, CDO at Mahindra Holidays and Anjali Malhotra, CDO at Aviva India.

"Not all digital is digital transformation," he reiterates.

The second category consists of organizations where huge white spaces exists that can benefit significantly through application of tech; i.e. ICT has not been applied to those operational processes. The most common example is core manufacturing where application of technologies like IoT and robotics in plants is bringing about huge efficiency gains leading to significant impact on bottomline. In such organizations, digitalization, as they often call it, is actually about application of technology to new areas.

Dube says typically such organizations look for good IT people with significant exposure to the specific business. Most of the Vedanta Group companies such as Sterlite Copper, Sterlite Power and Sesa Goa are examples of such companies. All the CDOs are tech people but are not directly handling traditional enterprise IT. In Sterlite Copper, for example, the Head of IT reports to the CDO Amitabh Mishra, a career IT professional who has spent years in similar industries including in GE, a pioneer in Industry 4.0—the holy grail of all manufacturing companies at present.

The third, which many refer to as the real transformation, is where digital transformation is about organizational change management, digital being just a lever. The actual task is integration of various functions and processes with target outcomes being significant shifts such as huge efficiency gains across organization (as opposed to specific processes in the above case), new revenue streams or even completely business model shifts. At the core of this transformation is culture shift.

Organizations taking this route usually prefer core business people who do not just understand the business but have "been there, done that" to drive the journey. Of course, they are executives with a mindset to innovate and are comfortable with disruptions; very often with a good sensitization about big changes happening to technology landscape.

Examples include Nischal Gupta of Sterlite Tech; Sarajit Jha, Chief Digital Value Acceleration at Tata Steel; Ritesh Pai at Yes Bank and the CDOs

Nischal Gupta
Chief Transformation Officer, Sterlite Tech

"60-70% of the transformation journey is actually about bringing a culture shift.'

in most insurance companies.

Theoretically, these could even be smart IT people who understand the business, both at an operational and strategic level and have the above skill and mindset attributes. At this point, however, very few of the actual leaders leading this kind of transformation hail from enterprise IT background.

There are exceptions, though. Companies where outlook towards technology is mature and organizational culture shift is not a huge part of the overall brief—like tech companies, online businesses, private banks—good enterprise IT managers are often entrusted with the task. Both Anjani Kumar, CDO of Collabera and Mandar Marulkar, CDO of KPIT (both IT companies) have enterprise IT background. And both of them still handle enterprise IT for their organizations, fully or partially.

However, as pointed out earlier, these industries are exceptions, rather than the rule.

India, Inc. has actually discovered its own sweet spots to source this kind of talent. The tech-leveraged start-ups and India's large tech companiesare good breeding grounds for digital leaders with just the right balance of skills and understanding. Gupta of Sterlite Tech actually came from Flipkart; Aarthi Subramanian, CDO of Tata Group has run line business in TCS and Jaspreet Bindra, ex SVP, Digital Transformation of Mahindra & Mahindra spent years at Microsoft.

Gap Analysis: Why so few CIOs handle digital transformation?

The idea that CIOs are the natural driver of digital transformation is rooted in a superficial understanding of the concept of digital transformation, which identifies it with technology. Over the period, it has been strengthened largely by the technology vendor community who use it to pitch their products. Most CIO forums and discourses are also based on this implicit assumption. The fact that most CIOs today are far more business savvy than ever is used to support this proposition.

As the data of CDOs and transformation heads show, this is clearly not the case. Very few CIOs actually drive digital transformation.

Our recent research for sister publication CIO&Leader on digital transformation in large Indian companies provides some of the possible explanations. We say possible because 'whether CIOs should drive transformation' was not an explicit research question. Our focus was on understanding the transformation at the ground level.

Here are some of the findings that can point to an answer.

The shift to Outside-in regime. Traditionally, tech has been applied to solve an existing business problem/requirement. In the digital era, where the transformation is essentially digital leveraged, it is the other way around. Look for new tech, quickly gauge if it has a scope to make big changes to your business, articulate that and convince the top management of the value that it can add to your business and how. 'How' has a fancy name: use case. So, in that sense, it is technology first. And the approach is outside-in.

Ironic as it may sound, this is what many see as loaded against the CIO. Traditionally, you have a business requirement which tech can help fulfil. So, the CIO is either given a clear-cut problem statement or in best of cases, he can work that out based on his interactions with various executives. But he needed that problem first to proceed. It is the classic inside-out.

It is not difficult to figure out these two require very different types of thinking. The best CIOs have been master problem solvers, who also understand business thoroughly but their ability to draw on blank canvas is unproven. For a successful line business manager, on the other hand, it has always been grabbing the opportunity present, without waiting for a clear definition.

Risk-taking is core to a CDO's role. Ability to take risk was pointed by most practitioners and consultants as a key requirement for the CDO.

"The CDO has to do a lot of new things, new innovations, often unproven, many of which may fail," says Dube of Russell Reynolds.

"The CIO's mandate is to run business-as-usual as reliably as he can. Even a small failure may bring business to a standstill," he says. This means as much de-risking as possible.

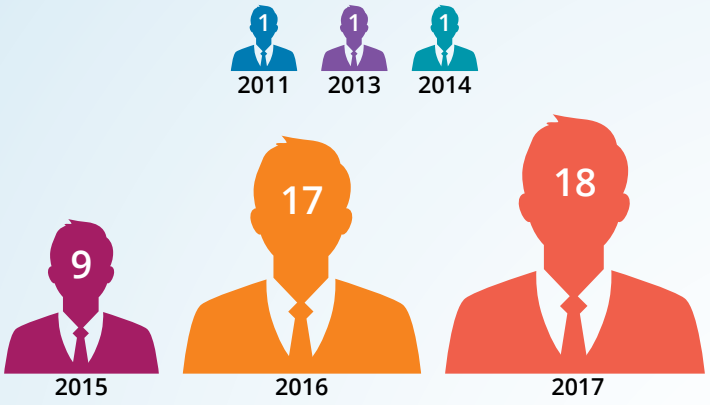
So, another perceived gap is the gap in mindset, specifically when it

Understanding India's CDOScape

Based on analysis of 44 Chief Digital Officers (CDOs) in India, Inc. at the end of 2017, this provides an insight into the demography of Indian CDOs.

Hiring of CDOs

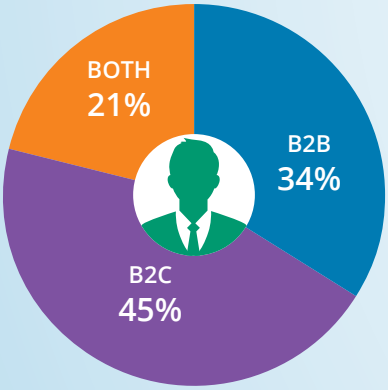
With the total base still very small, the growth that was seen in 2016 was not sustained in 2017. It was a flat growth. This shows number of CDOs hired and not net additions.



Source: 9.9 Group Research

CDOs Employed by Type of Business

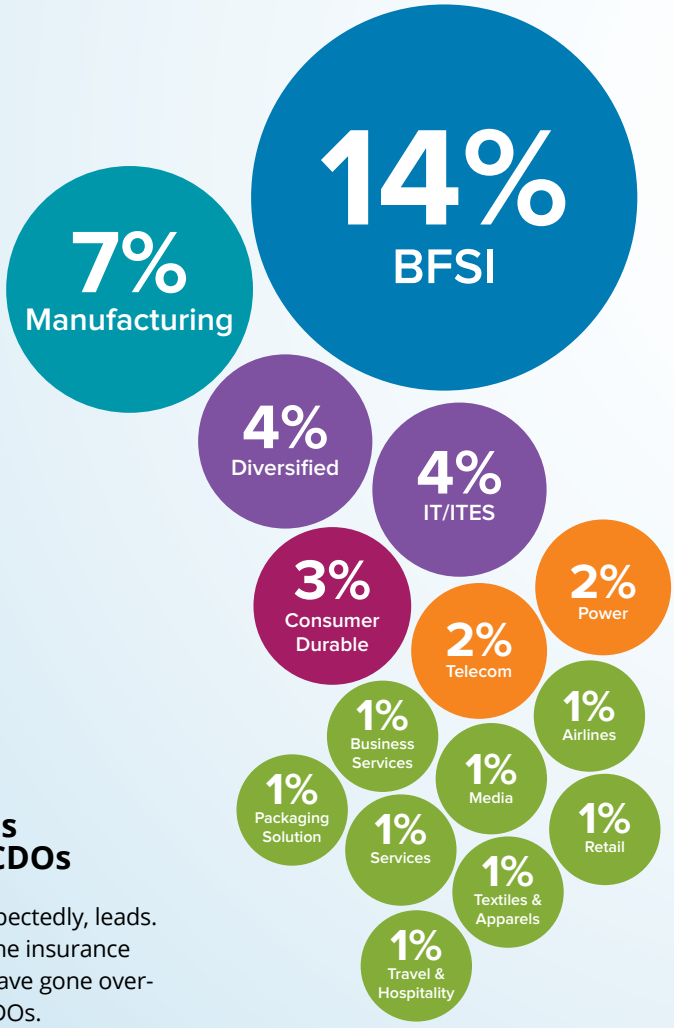
Expectedly, B2C businesses lead but B2B businesses are not far behind. Many diversified group CDOs lead for the group, consisting of both B2B and B2C businesses.



Source: 9.9 Group Research

Top Verticals Employing CDOs

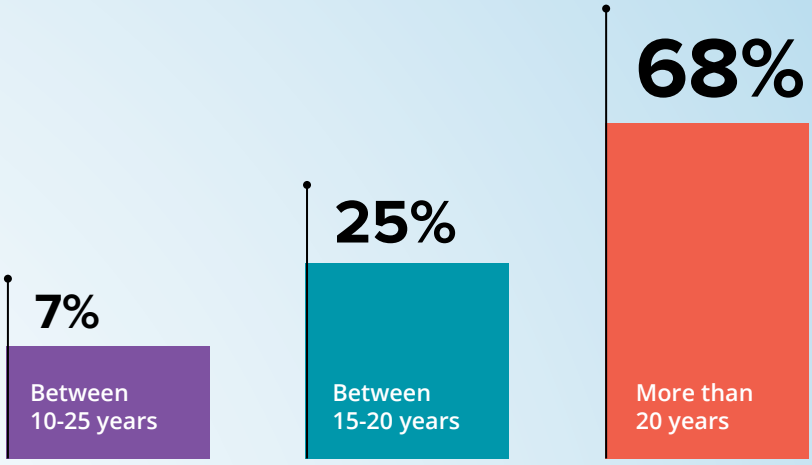
BFSI, not so unexpectedly, leads. Within BFSI, it is the insurance companies that have gone overwhelmingly for CDOs.



Source: 9.9 Group Research

It is at Fairly Senior Level

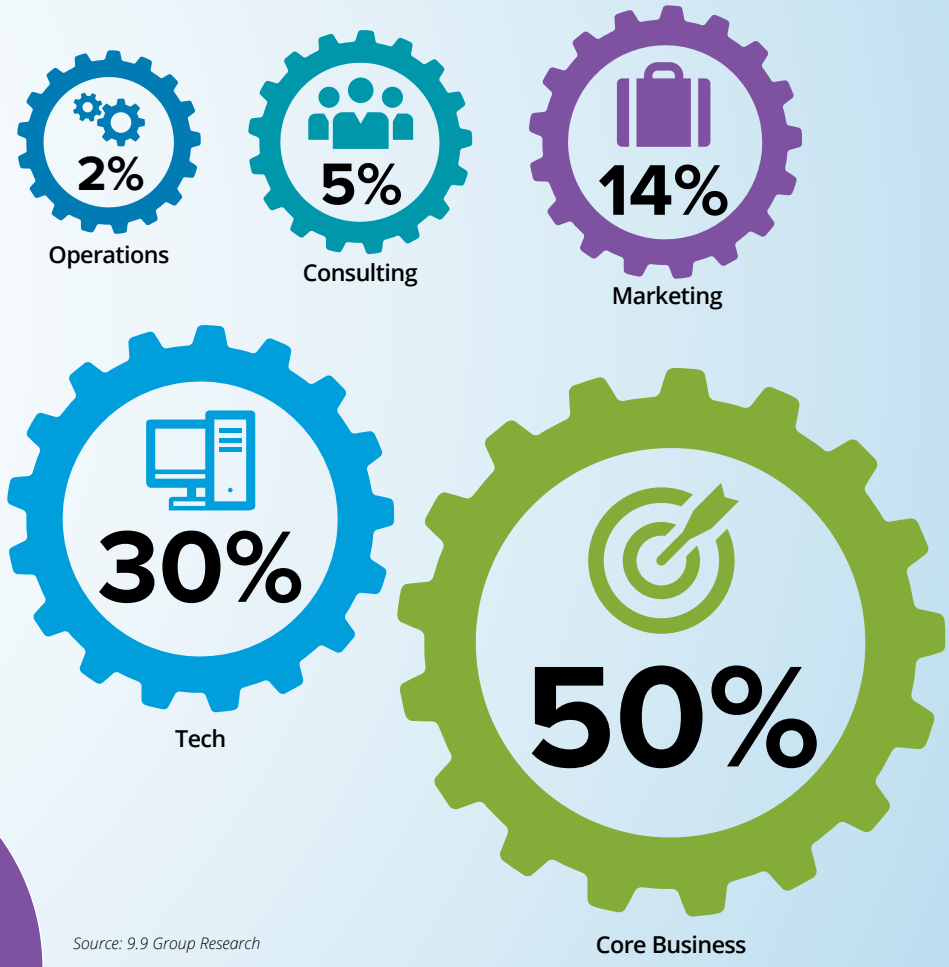
Organizations are entrusting their digital transformation task on fairly senior executives. Seven out of ten have more than 20 years of experience and 95% have more than 15 years of experience.



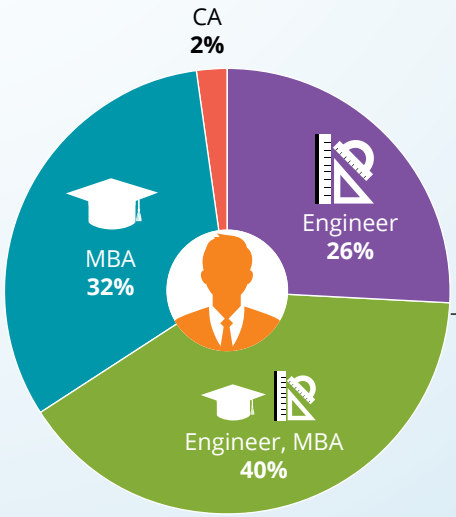
Source: 9.9 Group Research

Tech or Marketing? It is the Core Business Guys

As Enterprise IT and Marketing debate who is better suited for leading transformation, it is core business people who lead among digital leaders. Especially with organizations going for organizational change involving people, process and technology, it is the people who understand the business as well as change management are entrusted with the task.



Source: 9.9 Group Research



No worry, India has a lot of engineer-MBAs

Almost 98% are either engineers or MBAs or both.

Jaspreet Bindra
Advisor, Digital Tansformation, Mahindra & Mahindra

"A good digital leader must be exposed to design thinking, must be willing to take risks and should be a storyteller."

comes to risk taking.

It is the CIOs themselves. One of the few points on which there seem to be a near-complete consensus among digital leaders, other CXOs and consultants is that only a senior, dedicated executive can drive digital transformation.

'Dedicated' is the keyword here. The current thinking is that driving digital transformation is a full-time job. It cannot be just another KRA for some executive!

It is not too difficult to explain why. A typical transformation journey, especially in a traditional business, could involve a lot of time and focus to prepare the organization before it could leverage technology.

"60-70% of the transformation journey is actually about bringing a culture shift,' says Nischal Gupta, Chief Transformation Officer at Sterlite Tech. Almost all executives we spoke to identified culture shift as the toughest part of the transformation journey that requires undivided attention.

That can be manifested in a lot of discussion with other C level executives, creating communication programs for all employees, branded programs and a lot of similar stuff. The organizations are not convinced that an executive who is also monitoring a datacenter migration or fire-fighting a ransomware attack could effectively have the kind of focus that transformation requires.

Gupta of Sterlite Tech says one of the specific objectives of their transformation journey is "to free up the minds of every leader to focus on value addition rather than getting stuck in the business as usual in the day-to-day basis."

How can you do that, if you yourself are stuck in business as usual?

What it means is: A CIO cannot be entrusted with digital transformation while he is still in charge of datacenter rollouts or enterprise software implementation or laptop purchases.

Unless CIOs are willing to give up that role, other debates about their competences and skills are meaningless. A dedicated resource is a non-negotiable requirement from the CEO and board. Digital transformation is not a task. It is the single-most important initiative for an organization choosing that path. It cannot be handled along with datacenter rollout.

But why are the CIOs so keen on continuing with the nuts and bolts? "Many, for some reason, think their importance in the organization is directly proportional to the budget they handle," says a CIO-turned-consultant.

Despite being well-sensitized to the fact that their real contribution comes from business value they create, many CIOs cannot just think of giving up on their traditional role to take the new challenge.

So, while there are organizations that have people with enterprise tech background heading the transformation role, they are not in-charge of enterprise IT – the IT for business as usual.

Closing the gap

The new generation of IT leaders who are beginning to take over from the older generation of CIOs do not come with that mindset baggage that budget is everything. Their grasp of business is far better. And their generation, as a generic attribute, is far more willing to experiment. So, they can be good risk takers too.

The continuous sermonizing by the seniors that they need to be business savvy makes many feel defensive about tech. The new regime requires them to be proactively tech savvy, not just understanding technology but hunting for new technologies with full understanding of their own business to figure out if it can add value. They need not fall in love with one technology and make it work somehow. The organizations still need such people who will do so. Don't worry, enterprise tech will change too.

Becoming A Good Digital Leader

The Attributes

1. Must be innovative
2. Must be comfortable with disruption
3. Must be willing to take risk
4. Must be a good influencer

Maneesh Dube,
Consultant, Russell Reynolds

The Skills

Hard skills

- Exposure to digitalization areas; new tech, not just legacy tech
- Ability to develop use cases
- Entrepreneurial experience
- Understanding of new tech like IoT, ML, Big Data, Blockchain

Soft Skills

- Exposed to design thinking
- Comfort with agile way of working
- Tolerance for failure
- Risk taking
- Must be a storyteller
- Change Management skills

Jaspreet Bindra,
Digital Transformation Advisor, Mahindra & Mahindra

Practical Advice

1. Understand your business, industry landscape, competition
2. Keep updating yourself on tech; keep reading, subscribe to some good newsletters
3. Keep experimenting; start small
4. Always keep looking out (not just the big tech trends but what is happening around you)

Anjani Kumar,
Global CDO, Collabera

Anjani Kumar, CDO of Collabera, who himself moved from an Enterprise IT role to CDO role has the following advice. "Understand your business, do innovative thinking, do not be afraid of experimenting," he says adding that they must also be "customer advocates."

"If you understand business, understand technology and genuinely become a customer advocate within the organization, there's a fair chance that you would be a good digital leader," says Kumar.

It is difficult to cope with the fact that you will have to willingly dilute your 100% track record that resulted in your fast-tracking. Because, with unproven tech and newer business models, if you have a 100% success record, you have either been lucky or you have not tried enough. Few in corporate life will go by the first conclusion.

In short, all you need to realize is what brought you here will not take you there.

Attributes & Attitudes

We asked the practitioners as well as other stakeholders what are the skills and attributes of a good digital leader.

Here are some of the common traits that came out.

Maturity

1. They need not underestimate the value of tech in business
2. They must not overestimate the value of tech in business
3. They must be willing to 'let go'. Obstinacy may be a virtue for a basic researcher, not for a digital leader

Culture & Change Management

4. They must be restless about status quo; must be change agents
5. They should understand their organizational culture well
6. They must understand the relationship among people, process and tech and realize that all changes start and end with people
7. They must have excellent interpersonal skills (i.e good at relationships, not making impressive power points)

Risk-taking

8. They must be comfortable failing once in a while

Outside-in

9. They must understand—and continuously update themselves—about how tech landscape is changing
10. They must understand basic business dynamics fairly well and understand their own industry very well

Strategic Ability

11. They must be good design thinkers
12. They must be comfortable with chaos and haziness

As you may notice, some of these—probably everything other than risk taking—are desirable attributes of a CIO too. Quips Kumar, "Well, the desirable qualities of a good new generation CIO are the essential qualities of a CDO."

We could not have summed it up better.

Endnote

The digital game has just begun. Smart IT managers still have a chance to grab the opportunity. Knowing what they have achieved over the years, there is little doubt that they can acquire new skills needed for the new era.

Whether we see enough digital leaders, from among the IT leaders, rests then, on one major variable: their ability to let go. Their ability to defy gravity ■

EXTRA Curricular

Henry Potsangbam at one of his public speaking events

Speak Up

NEXT100 Winner 2017 **Henry Potsangbam**, Senior Manager, CDC Infra, Bharat Petroleum Corporation Limited (BPCL), talks about his passion for public speaking. He also shares various activities and achievements with regards to storytelling.

"Speech is power: Speech is to persuade, to convert, to compel."
– Ralph Waldo Emerson

Speaking publicly is both a challenge and an opportunity in itself. Some are in-born with it while some develop over time. Well, I fall in the second category.

I was never a confident speaker. In fact, I was very shy in my childhood. Even in my school in Manipur, I didn't talk much. There were talent search programs in my school where it was compulsory for everyone to participate and perform something on stage. However, I would be very scared to partake and avoid them.

However, gradually, this fear started evaporating when I moved to Delhi for high school. There, I started observing my fellow classmates and teachers, their communication skills, gestures, etc. Thereafter, I started speaking to them and slowly gained confidence. Having seen them participate in school fests, I also felt the need to try out something new. This urged me to indulge in the art of storytelling.

I started taking part in storytelling competitions. However, there was not much luck initially

Henry Potsangbam *Snapshot*

Henry Potsangbam is Senior Manager, CDC Infra at Bharat Petroleum Corporation Limited (BPCL). He is a winner of NEXT100 Award in 2017. He has done his Bachelors in Engineering & Technology. He holds numerous certifications from IBM and SAP and has worked in various levels at BPCL.

as I wasn't very confident on my public speaking abilities. It all changed for me in my engineering college in Maharashtra where I got an opportunity to speak about personal life and I did that confidently. Thereon, I participated in inter-collegiate competitions and received accolades – both from faculty and peers. After my transition from academic to professional life, I participated in storytelling competitions held at various IT forums and won prizes, which further boosted my confidence.

One of the highlights of my early public speaking days was when I organized "The Art of Storytelling" workshop, which focused on 'motivating ourselves to do better personally and professionally'. People started familiarizing with the story. I won another prize, this time at an event organized by my company. I still get invites from my school and college to speak on motivational topics, which I speak happily.

Henry Potsangbam in his public speaking mode

Henry Potsangbam's speech at a public speaking workshop organized by his company:

"Now I feel pride in taking my own decisions. From that day, never have I repented and looked for any reasons, even in times of failure. Because I own my decisions however hard or tough they are! I always have the liberty to make a conscious decision."

"I am telling this story not for anyone else, but me. I am here today because I choose to be. I will be there tomorrow because I decided it today."

Majority of my storytelling focuses on the dreams and ambitions of people have and how they can accomplish them. It primarily revolves around inspiring yourself to achieve what you want in life.

Some of the key leaders who have inspired me as a speaker include Martin Luther King Jr. and Robin Sharma. Especially, Martin Luther King Jr.'s speech -- *"I have a dream today. I have a dream that one day every valley shall be exalted, every hill and mountain shall be made low, the rough places will be made plain, and the crooked places will be made straight, and the glory of the Lord shall be revealed, and all flesh shall see it together."* – was truly inspiring to me. I attended a speech by Robin Sharma where he made the non-listeners pay attention to him. The stand-up shows are a lesson for all of us on how to keep the audience engaged for a length of time ■

As told to Dipanjan Mitra, Content Executive-Enterprise Technology, ITNEXT

Securing The Digital Supply Chain

Encryption of data and end-point devices provides the last line of defense in a digital supply chain

By Rahul Kumar

Ensuring a secure supply chain is a necessary precondition in today's world of commerce. The digital supply chain has emerged as the weakest link for the potential insertion of malware backdoors. Governments and industry are just getting around to addressing the various concerns relating to supply-chain security.

When it comes to data security challenges, human and technological influences can be amongst the most difficult to manage, seriously exacerbating cyber risk to IT-enabled supply chain management (SCM). It is quite common to find SCM software running on top of business software, exposing organizations to myriad risks and attacks. In fact, digital supply chain risks keep evolving with technological advancements and there is no end in sight for a definitive solution to address them. Merely determining the authenticity of various hardware, firmware and software components does not guarantee a secure system.

80% of data breaches begin here

It is common knowledge that most of the companies do not have full visibility into their supply chain. In fact, the potential risk exposure of a company increases with the number of unmanaged suppliers. It is quite normal for even a mid-sized firm to be part of a complex web of global inter-depen-

dencies that are driving synchronized commerce today. Technological disruption has made the digital supply chain the prime source of risks, although there are several other ways that an organization could suffer a compromise leading to information theft or a service outage.

With organizations relying on software and services from third-party providers, the risk of exposure to cybercrime gets only higher and supply chain disruptions are becoming costlier. It is estimated that 80% of all information breaches originate in the supply chain, with manufacturers facing the brunt of all attacks—mostly from unplanned IT or communication outage, followed by cyberattacks and data breaches. The digital supply chain is also the favored arena for malicious actors to plant malware, to devastating effect. Remember what happened when several Chrome extensions were compromised? It resulted in hijacking of traffic and exposing users to potentially malicious pop-ups and credential theft.

Risks exist at every stage

Cyber supply chain risks may originate at the suppliers' end (inclusion of unwanted functionality, data or network breaches, insider threats); at the place of business operation (data theft or alteration of data, insertion of malicious software and hardware, outages, etc.); or at the distribution end (theft, tampering, counterfeiting, etc.). Many functions, departments and roles in an organization own the risks affecting supply chain security. Risk blind spots in the supply chain occur only when little or no communication or cooperation takes place—both inside and outside of an organization.

It is, therefore, important to formulate a strategy for end-to-end risk management in the supply chain, ensuring its integrity, security, and resilience. A successful strategy should outline ways to secure the organization and its dependencies, covering all tiers in the chain. The continued ascendancy of supply chain risks has led to the evolution of new risk management approaches, which focus on existing cybersecurity and supply chain practices for building an effective digital supply-chain.

By identifying vulnerable systems and components, businesses can formulate risk mitigation measures that are cost-effective and efficient

Rahul Kumar
Country Manager, WinMagic

By identifying vulnerable systems and components, businesses can formulate risk mitigation measures that are cost-effective and efficient. Organizations can keep information assets secure by adopting and applying standards such as ISO 27000 and 31000, and recommending the same to all the players in the supply chain. This would require the implementation of technology and process upgrades, encryption, access policies, intrusion prevention systems, and other key best practices. It also makes sense to have a core group of risk owners collaborate on administrative and operational affairs, which also have a direct or indirect bearing on supply chain security. For instance, it is particularly important to immediately communicate any personnel changes to supply chain partners so that account profiles can be updated.

Businesses can change for the better when they realize that the cyber-security of any one organization within the chain is only as strong as that of the weakest member. With information and security practices shared across a supply chain, continued effort on the part of all stakeholders can convert their weakest link into an asset. Encryption of data and end-point devices provides the last line of defense in a digital supply chain. Of what use is the best technology or practice if an organization's staff or those in supplier organizations still are fooled by phishing attacks? Just one misplaced click could affect millions of consumers, bring down the organization's reputation, impact revenues, and even risk business continuity. Securing data and devices with encryption across the enterprise and supply chain networks is a great means of protecting the enterprise against attacks, threats, and other risks—whether malicious or unintentional ■

A Framework For Future-Proofing Backup And Recovery

The framework can help you to ensure maximum ROI on your investment

By Ajay Ahuja

Experts predict that most enterprises will experience a 50x data growth by 2020. Yet many companies are still taking a traditional and generic approach when it comes to backup, recovering and retaining ever-growing amounts of data. The result is sprawling data sets and backup systems, leading to substantial risk of data loss and inability to recover in a timely manner. So how can organizations protect the business data that resides in their mission critical enterprise databases?

Data is the new engine powering the global digital economy, so much so that the insights it unlocks are considered a key source of competitive advantage and are even seen as a form of data capital. Conversely, any compromise of customer-facing databases, loss of enterprise data or downtime of business applications can be catastrophic to a company.

The challenge is that unexpected outages and the increasing number of cyber-attacks can cause data loss and corruption. It is essential that a company's mission critical enterprise databases are protected and that timely and accurate data recovery is available to ensure near-zero business disruption.

Yet numerous enterprises are still stuck with archaic data backup and recovery mechanisms. These cause long backup windows, unnecessary overhead on database servers, virtually no insight into recovery capability, unpredictable restore performance and little knowledge as to whether or not backups are valid. The ever-expanding data universe is only making things worse.

So how should companies protect critical databases?

Modernize your backup and recovery strategy

Database-aware, engineered protection

Organizations are recognizing that there are important data protection differences between data types

- for example, flat files consisting of single tables of data, commonly used to import data in data warehousing projects versus relational databases. Consequently, they are moving towards specialized, application-aware solutions for critical data instead of the traditional generic, one-size-fits-all approaches. One such example is Oracle's Zero Data Loss Recovery Appliance. The resulting code level integration with the transactional databases for data protection delivers the end-to-end visibility and automated backup validation, simplifying management and reducing risk to the business.

The results can be quite impactful. Take, GE Aviation, for example. This US based global aircraft manufacturer wanted to create what it refers to as its resilience platform for its new ERP system. The company wanted to reduce the long recovery windows experienced with its legacy system to bring critical systems back online as quickly as possible. As a result, recovery times were reduced from about 20 hours down to 2 hours – a 90% faster database recovery!

To add to the delight, the enterprise achieved an immediate Return on Investment (ROI) by reducing the risk of data loss with a Recovery Point Objective (RPO) of less than a second versus hours. The company also gets peace of mind with end-to-end backup validation without any overhead on personnel or database servers. Effectively, GE Aviation went from "assuming" backups could be successfully restored to knowing current status for all of the protected databases under management.

In addition to the better system performance, they have also been able to change and improve their entire operating procedure, and the project lead knows there won't be any 3 AM calls!

Other companies like AMMROC, a world class military maintenance company, achieved 32x faster backups and 8x faster recovery, enabling the company to provide 24x7 maintenance, repair and overhaul services to its customers without delays.KEB Hana cards, a Korean credit card company, achieved 13x faster backups and a sub second recovery point objective, virtually eliminating data loss exposure and ensuring data security.

By identifying vulnerable systems and components, businesses can formulate risk mitigation measures that are cost-effective and efficient

Ajay Ahuja,
Director & Head - Systems Sales Consulting, Oracle India

So, for any new solution, and in order to ensure maximum ROI on your investment, you should consider this 5-point framework for future-proofing your backup and recovery engine.

1. Eliminate data loss – Look for tools and techniques to protect ongoing database transactions with the goal of sub second recovery.

2. Database level recoverability – Architect your database data protection strategy around recovery instead of just backups. For example, insist on automated monitoring and alerting allowing you to know, not guess, the current recovery window and data loss exposure for all databases, not just backup issues. Ensure that the solution provides end-to-end data validation, so you'll know that you have a good backup and not be surprised by data corruption when you need to recover.

3. Cloud-scale Architecture – Design for ease of management, reducing error-prone processes, with policy-based management leveraging one backup strategy across all databases. The solution should be highly available with no single point of failure and deliver linear performance with scale-out to meet data growth realities.

4. Compliance requirements – Incorporate database level policies with automated reporting, monitoring and alerts, protecting backups across their full lifecycle including disk backups, tape backups and remote replication. In addition, the solution should meet regulatory requirements for timely recovery - in some cases this can be as short as two hours -with no data loss exposure.

5. Minimal impact backup – Ensure all backup and recovery related processing, including tape backups (if needed) have minimal impact on productions workloads for backup processes such as backups, deduplication, purging of backups, backup validation, or compression.

Already, many leading global enterprises have started to rethink and redesign their backup and recovery strategies around this five-point framework. Is your organization ready to future-proof its backup and recovery engine? ■

Cloud Apps And Web Portals Most Vulnerable To Attacks

Gemalto's 2018 security survey indicates that more organizations have hired a dedicated CISO in the last one year

The mainstreaming of cloud and the use of a disparate range of devices within businesses has led to nearly two-thirds of IT decision makers admitting that their security teams are considering implementing consumer-grade access to cloud services for employees. Gemalto's 2018 Identity and Access Management Index Survey interviewed more than 1,000 IT decision makers globally and found that a majority of them believe that the authentication methods they implement in their businesses are not as good compared to those found on popular sites including Amazon and Facebook.

Recent high-profile data breaches are influencing businesses' security policies, with nine in 10 respondents admitting making changes as a result. In fact, the role of a dedicated Chief Information Security Officer within organizations has increased by a quarter in the last year, while 58% of businesses have implemented access management solutions to account for these concerns.

Nine in ten IT decision maker respondents state that their organization's security policies around access management have been influenced by breaches of consumer services, which shows how powerful these breaches can be.

Most vulnerable to attacks

Around 50% of respondents highlight web portals as one of the biggest targets, around two in five say the same for cloud applications (SaaS, PaaS, IaaS), 39% mobile applications, 37% local network access and just under three in ten say so for VPN. In addition, two fifths of respondents consider unprotected infrastructure such as IoT to be a big target for cyber-attacks.

Over four in ten respondents see cloud applications as one of the biggest targets for cyber-attacks. Of these respondents, 71% indicate the reason behind this may be the increasing volume of cloud applications in use, and 55% say that the lack of strong cyber security solutions to implement appropriate solutions. Over two fifths also indicate cloud applications may be targeted for cyber attacks because access management solutions are currently in place for the cloud are poor, which is something that organizations could improve.

Two-factor authentication is gaining adoption

The vast majority of respondents' organizations are now using two-factor authentication for at least one application. For instance, eight in ten respondents report that their organization has at least one application that is currently protected by two-factor authentication for cloud applications (SaaS, PaaS, IaaS), 78% for local network access and web portals, with 77% for VPN and enterprise applications.

Spend more on security

A total of 45% respondents agree that their companies have started spending on access management (45%), staff being trained on security and access management (44%), and more resources being allocated to access management (42%). In addition, around two in five say that secure access management is now a priority for the board, rising slightly from 34% in 2016.

Despite social platforms having been used in the past as an attack route for malicious actors to breach organizations, it seems IT departments fall short in being able to apply cohesive access security for social platforms

The impact of social media

The survey also highlights the extent to which social media platforms play a role in marketing. Interestingly, despite social platforms having been used in the past as an attack route for malicious actors to breach organizations, it seems IT departments fall short in being able to apply cohesive access security for social platforms. For example, over two fifths indicate that employees use a company-approved individual account when using social media for work. According to the survey, 50% of respondents report that their organization secures access to its social media accounts via a relatively simplistic method of username and password, a slight drop from the 65% who reported doing so in 2016. There are of course, those who say that their organizations use native two-factor authentication provided by social media sites.

Compliance and auditing

Nearly all respondents think that two-factor authentication will be able to contribute towards their organization's ability to comply with data protection regulations and pass security audits, with over half believing that this is definitely the case. Similarly, the majority of respondents believe that it is important that their organization is able to produce a single audit trail of access events taking place throughout different resources used by the organization, with nearly three in ten viewing this as extremely important. The ability to encourage better compliance and easier auditing may not often be the primary reason to implement two-factor authentication, but is certainly an added bonus ■

India Leads China In Enterprise Application Software Spending

Increased competition, alignment of IT to business and rate of technology change are some of the reasons for increased spending

Enterprise application software spending in India will reach USD 2.5 billion in 2018, a 19.8% increase from 2017, according to Gartner. In China, 2018 enterprise application software spending will reach USD 5.1 billion, a 18.9% rise from 2017.

While both countries are poised for continued growth, organizations have different criteria for selecting the vendors they use. For example, a recent end-user survey by Gartner showed that corporate branding is an important software

selection criterion in China, while organizations in India focus more on pricing and contract flexibility.

"China's and India's enterprise application software spending has grown at double-digit rates historically, and they will continue to be hot spots," said Keith Guttridge, research director at Garner. "To be competitive in those countries, technology business unit leaders in technology providers must understand software adoption dynamics and spending intentions."

Hot spots for growth

Survey respondents were asked how they anticipate that spending on enterprise applications will change in 2018. The survey found that India's spending intention is more aggressive than China's. In all categories, India has a higher percentage of respondents who want to increase spending across all enterprise applications. Enterprise content management (ECM), business intelligence (BI), customer relationship management (CRM) and open source (enterprise edition) were the most popular in India. In China, the most popular were open source, ECM and CRM.

"Although ECM is considered a hot market, it remains small in terms of share. However, as organizations in emerging countries are growing rapidly and business requirements becoming increasingly complex, there is increasing demand for solutions to digitalize content to support business processes as part of digital workplace initiatives," said Guttridge. "CRM is claiming some budget spending intention from other major applications, such as ERP, while open-source applications continue to have a good proportion of increased spending intentions."

Reasons for increased spending

Although transforming to digital business is an important reason to increase software spending, other factors take precedence in the survey results. Respondents suggested practical reasons for increasing software spending in 2018, including increased competition, alignment of IT to business and rate of technology change. In India, increased competition and availability of skills are other top reasons for increased spending. In China, many end-user organizations are struggling to keep up with fast-growing customer requirements, and must invest in their rapidly expanding customer bases.

Key initiatives for software spending

In India, increased software spending is being strongly influenced by overarching digital transformation (chosen by 91% of respondents), followed by mobile (88%) and artificial intelligence (88%). In China, cloud/SaaS offerings lead as the top influencer (chosen by 63% of respondents), followed by Internet of Things (IoT — 62%) and mobile (60%).

IoT is particularly significant in China due to the large manufacturing base, and the fact that "smart manufacturing" is an official initiative in the country's 13th Five-Year Plan. However, adoption of emerging initiatives, such as IoT, AI and digital transformation will largely vary. Some end-user organizations are still piloting, experimenting with and trialing their own resources in order to implement these initiatives.

"Despite moderate economic growth, technology and service providers (TSPs) should craft a go-to-market strategy that assumes that China and India will continue to be fast-growth markets in the region and the world," said Guttridge. "TSPs can differentiate their offerings by providing 'hand-holding' mini-consultations for key initiatives, such as IoT (especially in China), AI and digital transformation (especially in India). They can also deliver use-case scenarios that demonstrate the value of products and services to these emerging technologies." ■

India Worst Hit By Ransomware

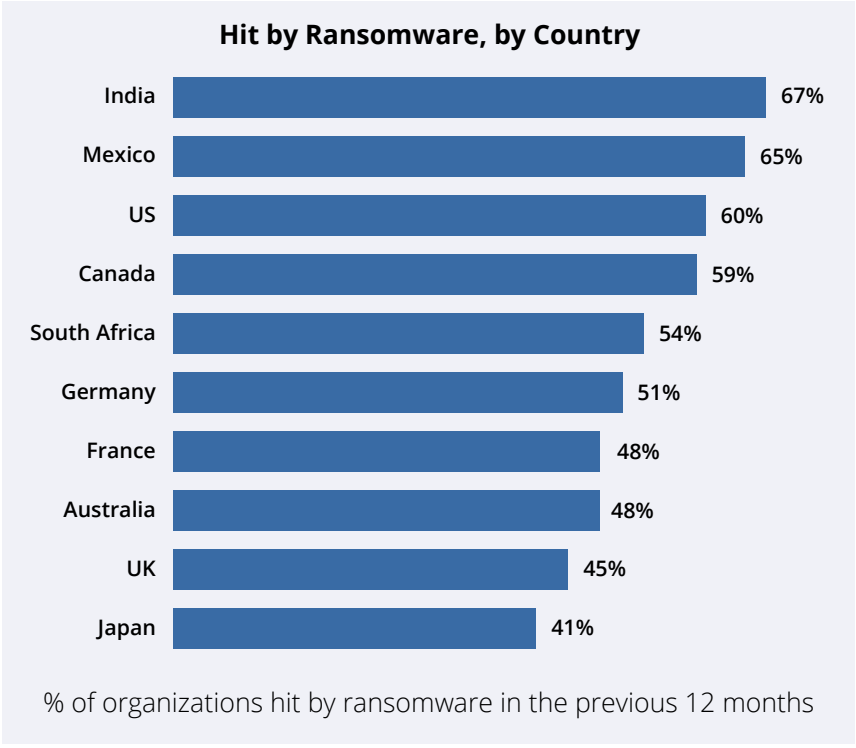
Despite the intensity and magnitude of attacks, Indian businesses are still not prepared to defend itself against determined attackers

Indian businesses are at a risk of repeated ransomware attacks and are vulnerable to exploits, according to Sophos' India findings of its survey, *The State of End-point Security Today*. The survey polled more than 2,700 IT decision makers across mid-sized businesses in 10 countries worldwide, including the US, Canada, Mexico, France, Germany, the UK, Australia, Japan, South Africa and India. The survey concludes that despite the intensity and magnitude of attacks, Indian businesses are still not prepared to defend itself against determined attackers.

Ransomware continues to be a major issue across the globe with 54% of organizations surveyed hit in the last year and a further 31% expecting to be victims of an attack in the future. On average, respondents impacted by ransomware were struck twice. India is the worst hit (67%) among all the surveyed countries, as seen in the Figure.

"Unlike lightening, ransomware can strike again and again to the same organization. We're aware of cybercriminals unleashing four different ransomware families in half-hour increments to ensure at least one evades security and completes the attack," said Sunil Sharma, Managing Director Sales at Sophos India & SAARC. "Today's persistent cyber-criminals are deploying multiple attack methods to succeed, whether using a mix of ransomware in a single campaign, taking advantage of a remote access opportunity, infecting a server, or disabling security software. If IT managers are unable to thoroughly clean ransomware and other threats from their systems after attacks, they could be vulnerable to reinfection. No one can afford to be complacent."

This relentless attack methodology combined with the growth in Ransomware-as-a-Service, the anticipation of more complex threats, and the resurgence of worms like WannaCry and NotPetya puts businesses in serious need of a security makeover,



according to Sophos. In fact, more than 90% of Indian IT decision makers surveyed impacted by ransomware were running up to date endpoint protection, confirming that traditional endpoint security is no longer enough to protect against today's ransomware attacks.

According to those impacted by ransomware last year, the median total cost of a ransomware attack was USD 133,000. Indian organizations median total cost stood at USD 1.17mn, the highest, in rectifying the impacts of ransomware. This extends beyond any ransom demanded and includes downtime, manpower, device cost, network cost, and lost opportunities.

Two-Thirds of IT Admins Surveyed Don't Understand Anti-Exploit Technology

IT professionals also need to be aware of how exploits are used to gain access to a company's system for data breaches, distributed-denial-of-service attacks, and cryptomining. Unfortunately, Sophos' survey revealed considerable misunderstanding around technologies to stop exploits with 72% unable to correctly identify the definition of anti-exploit software. With this confusion, it's not surprising that 45% do not have anti-exploit technology in place at all. This also suggests that a significant proportion of organizations have a misplaced belief that they are protected from this common attack technique yet are actually at significant risk.

IT professionals also need to be aware of how exploits are used to gain access to a company's system for data breaches, distributed-denial-of-service attacks, and cryptomining

Intrusions from exploits also have been happening for years but are still a prominent threat and often go undetected for months, if not years. Once inside a system, cybercriminals use complex malware that can hide in memory or camouflage itself. In many cases, businesses do not know they've been breached until someone finds a large cache of stolen data on the Dark Web.

"It's time to disrupt these intrusions," said Sunil. "Since traditional endpoint technologies are often unable to keep up with advanced exploit attacks used to compromise a system, Sophos has added predictive, deep learning capabilities to the newest version of its next-generation endpoint protection product, Sophos Intercept X."

Although 94% of respondents admitted their endpoint defenses need to be stronger to block the attacks seen last year, only 34% have predictive threat technologies, such as machine or deep learning, leaving 66% vulnerable to repeated ransomware attacks, exploits, and evolving advanced threats. 63% plan to implement predictive threat technology within a year, yet confusion about it persists. Of those surveyed, 37% admitted that they do not have a full understanding of the differences between machine learning and deep learning.

"Given the speed at which IT threats are evolving and becoming more persistent and coordinated, it is a deep concern to see the adoption of the next-generation predictive technologies. It is important for organizations to keep up in this dynamic world of IT threats. Organizations need effective anti-ransomware, anti-exploit, and deep learning technology to stay secure in 2018 and beyond," said Sunil ■

Do Facebook Users Really Care About Online Privacy?

How many of 2 billion Facebook users are actually concerned about how their data is used by companies like Cambridge Analytica?

By Shubhra Rishi

Most of you may not have heard of the Baader-Meinhof Phenomenon. It is a phenomenon where you may come across an obscure piece of information - and soon afterwards encounter the same subject over and over again. Now think about your online browsing habits. Today contextual advertising allows advertisers to use your data and display them as ads on other websites. Now Facebook, like many other websites and mobile applications, collects a lot of data about you - information such as your name, age, gender, location, language, education, ethnic affinity, school, income, net worth, among other things. For years, it has tracked your on-site activity, storing information such as ads you click, pages you like, emotions you use to express your feelings on a post or a video, your location settings, among other things. And that's how you witness ads on your facebook page that are relevant and useful for you.

In 2017, Facebook's monthly active user base grew to over 2 billion. Facebook along with its other popular platforms, Whatsapp and Instagram, have approximately 60% penetration among internet users. The social

network has reported 47% growth in revenue to about USD 17.4 billion in the first half of 2017. The company is driven by solid growth in advertising and mobile ad revenues across geographies. Mobile ads now account for 87% of advertising revenues and stood at USD 8 billion in Q2, 2017.

In its data usage policy, Facebook has revealed what it collects from a user:

- Content and other information that you provide when you use Facebook for their services
- Information other people share about you
- Your networks and connections
- Your information about a purchase or transaction
- Your device and mobile operator information
- Information from websites and apps that use Facebook's services
- Information about you and your activities on and off Facebook from third-party partners

Since 2014, Facebook has a platform policy that clearly states what developers of third party apps can and cannot do. With regards to data, third party apps have to elaborate in their privacy policy on what data they are collecting and how they plan to use that data. These third-party apps must also delete any data received from Facebook. What Facebook also does now is moderate third party apps. Apps go through a review process where they must justify why that information is necessary for the app. Facebook characterizes "detailed information" as anything other than a user's friends, public profile, and email. Approval is only granted if apps can show that the information they requested will be directly used. But Facebook's updated platform policy only came into place a year after the "Cambridge University researcher named Aleksandr Kogan had created a personality quiz app, which was installed by around 300,000 people who shared their data as well as some of their friends' data," as revealed by Zuckerberg in the public post. In the post, Zuckerberg also added that before 2014, the social network "allowed access to a large amound of information" to third-part apps."

So what's so surprising about the recent Cambridge Analytica story? Wasn't Facebook built precisely to allow companies like Cambridge Analytica to do what it did? And how many of these 2 billion users are actually concerned about how their data is used by these companies?

Research has proven from time to time that users are finally waking up to care a little.

Take for instance, the 2013 revelation by NSA whistleblower Edward Snowden who told the truth about extensive US government surveillance of phone and internet data. Findings by Pew research found that Americans continue to have conflicting views about government surveillance programs. A majority of Americans (54%) disapproved of the US government's collection of telephone and internet data as part of anti-terrorism efforts and wanted to control their personal information, but few feel like they are able to. Most say it is important to control who can get their information (93%), as well as what information about them is collected (90%). But only 9% say they have a lot of control over how much information is collected about them.

A KPMG survey in 2016 also found that more that 82% of consumers are not comfortable with the sale of their data to third-parties. 55% said a free fitness tracking device that monitors the well-being of users and produces a monthly report for them and their employer is crossing the privacy line.

The survey also revealed that consumers have mainly top three concerns about the way organizations are handling and using their personal information were: unwanted marketing; personal information being sold on to third-parties, and lack of secure systems. The survey found that strong cyber security systems (32%) are the most effective thing an organization can do for customers to trust them with their personal data. Over half of survey respondents also said that they were willing to share their gender, education or ethnicity online, while a considerably lower proportion were happy to share more sensitive information, such as location (16%), address (14%) or medical records (13%). Looks like the consumers/users are already deleting their internet browser cookies or managing their social media settings. "Almost one-third even use incognito or 'do not track' modes, while a quarter percent use encryption," revealed the survey.

This is good news.

With the plethora of apps in your mobile appstore collecting personal information, what you plan to share or not share, is your responsibility. How marketers, advertisers or internet and tech companies use this information is largely public knowledge today. Informed users have a choice: they can either be smart about how they use these apps or be careful about what they reveal. Reminds me of a quote by famous author, Gabriel García Márquez, who once said, "all human beings have three lives: public, private, and secret." Maybe it's time to revisit what you share on social media ■

A KPMG survey in 2016 also found that more that 82% of consumers are not comfortable with the sale of their data to third-parties

Companies Are Not Confident About Complying With GDPR

The lack of a consistent CSIRP is a persistent trend each year

The General Data Protection Regulation (GDPR) takes effect in May 2018 and will mandate that organizations have an incident response plan in place. At least 77% of respondents said in a new study conducted by Ponemon Institute and sponsored by IBM Resilient, do not have an incident response plan that is applied consistently across the entire enterprise. Most countries surveyed do not report confidence in their ability to comply with GDPR. A report by research firm Gartner in November last year, also alluded to the fact that less than 50% of all organizations impacted will fully comply by the GDPR deadline of 25th May, 2018. The GDPR regulation levies steep penalties of up to EUR 20 million or 4% of global annual turnover, whichever is higher, for non-compliance. The language in the guideline uses the word "reasonable" to indicate the level of data protection and privacy that companies should observe towards EU citizens.

> One of the key factors impacting overall cyber resiliency include difficulty retaining and hiring IT security professionals

The study has also found that 77% of respondents admit they do not have a formal cyber security incident response plan (CSIRP) applied consistently across their organization. Nearly 50% of the 2800 respondents have said that their incident response plan is either ad hoc or completely non-existent.

However, 72% of organizations this year feel more cyber resilient in 2018 than they were last year. This confidence, the survey reveals, is due to their ability to hire skilled personnel. This confidence may be misplaced, with the analysis revealing that 57% of respondents said the time to resolve an incident has increased, while 65% reported the severity of the attacks has increased.

Some of the key factors impacting overall cyber resiliency include:

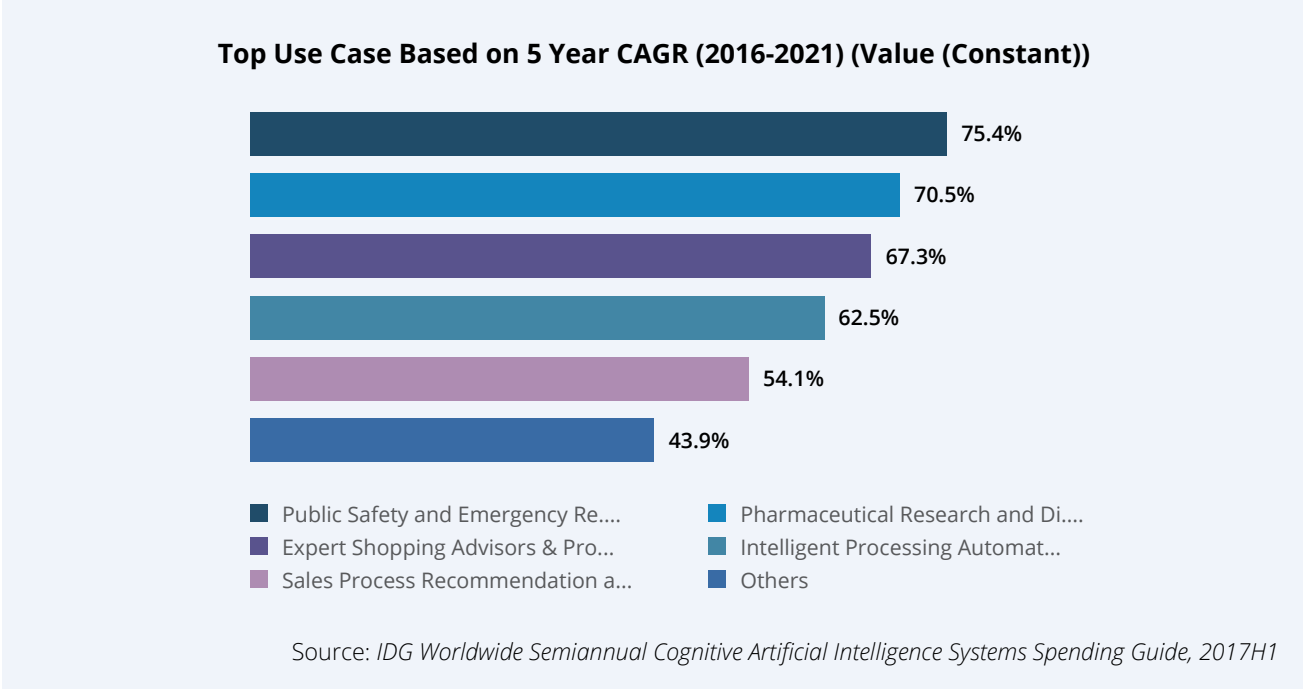
- Lack of an adequate cyber resilience budget in place (69%)
- Difficulty retaining and hiring IT security professionals (77%)
- Lack of investment in AI and machine learning as the biggest barrier to cyber resilience (60%)

The lack of a consistent CSIRP is a persistent trend each year despite a key finding from IBM's 2017 Cost of a Data Breach Study. The cost of a data breach was nearly USD 1 million lower on average when organizations were able to contain the breach in less than thirty days – highlighting the value and importance of having a strong CSIRP. The survey has found that these organizations have had a CISO in place for three years or less. 23% report they do not currently have a CISO or security leader ■

Global Spending On AI And Cognitive Systems To Rise

Cognitive and AI spending will grow to USD 52.2 billion in 2021 and achieve a compound annual growth rate (CAGR) of 46.2% over the 2016-2021 forecast period

Worldwide spending on cognitive and artificial intelligence (AI) systems will reach USD 19.1 billion in 2018, an increase of 54.2% over the amount spent in 2017. With industries investing aggressively in projects that utilize cognitive/AI software capabilities, the International Data Corporation (IDC) Worldwide Semi-annual Cognitive Artificial Intelligence Systems Spending Guide forecasts cognitive and AI spending will grow to USD 52.2 billion in 2021 and achieve



Source: *IDG Worldwide Semiannual Cognitive Artificial Intelligence Systems Spending Guide, 2017H1*

a compound annual growth rate (CAGR) of 46.2% over the 2016-2021 forecast period.

"Interest and awareness of AI is at a fever pitch. Every industry and every organization should be evaluating AI to see how it will affect their business processes and go-to-market efficiencies," said David Schubmehl, research director, Cognitive/Artificial Intelligence Systems at IDC. "IDC has estimated that by 2019, 40% of digital transformation initiatives will use AI services and by 2021, 75% of enterprise applications will use AI. From predictions, recommendations, and advice to automated customer service agents and intelligent process automation, AI is changing the face of how we interact with computer systems."

Retail will overtake banking in 2018 to become the industry leader in terms of cognitive/AI spending. Retail firms will invest USD 3.4 billion this year on a range of AI use cases, including automated customer service agents, expert shopping advisors and product recommendations, and merchandising for omni-channel operations. Much of the USD 3.3 billion spent by the banking industry will go toward automated threat intelligence and prevention systems, fraud analysis and investigation, and program advisors and recommendation systems. Discrete manufacturing will be the third largest industry for AI spending with USD 2.0 billion going toward a range of use cases including automated preventative maintenance and quality management investigation and recommendation systems. The fourth largest industry, healthcare providers, will allocate most of its USD 1.7 billion investment to diagnosis and treatment systems.

"Enterprise digital transformation strategies are increasingly including multiple cognitive/artificial intelligence use cases," said Marianne Daquila, research manager, Customer Insights & Analysis at IDC. "Business transformation is occurring across all industries as successful companies embrace the array and potential impact of these solutions. Automated customer service agents, increased public safety, preventative maintenance, reduction of fraud, and improved healthcare diagnosis are just the tip of the iceberg driving spend today. With double-digit year-over-year spending growth forecast, IDC expects to see an increase in general use cases, as well as a refinement of industry-specific use cases."

The cognitive/AI use cases that will see the largest spending totals in 2018 are: automated customer service agents (USD 2.4 billion) with significant investments from the retail and telecommunications industries; automated threat intelligence and prevention systems (USD 1.5 billion) with the banking, utilities, and telecommunications industries as the leading industries; and sales process recommendation and auto-

Retail will overtake banking in 2018 to become the industry leader in terms of cognitive/AI spending

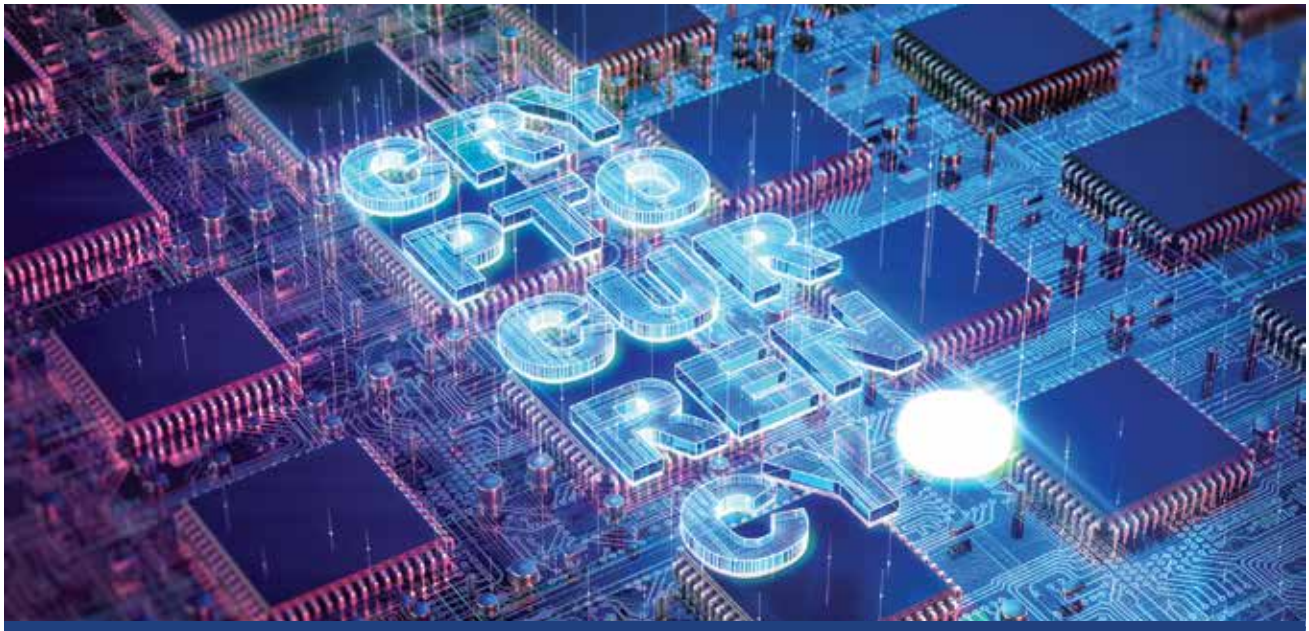
mation (USD 1.45 billion) spending led by the retail and media industries. Three other use cases will be close behind in terms of global spending in 2018: Automated preventive maintenance; diagnosis and treatment systems; and fraud analysis and investigation. The use cases that will see the fastest spending growth over the 2016-2021 forecast period are: public safety and emergency response (75.4% CAGR), pharmaceutical research and discovery (70.5% CAGR), and expert shopping advisors and product recommendations (67.3% CAGR).

A little more than half of all cognitive/AI spending throughout the forecast will go toward cognitive software. The largest software category is cognitive applications, which includes cognitively-enabled process and industry applications that automatically learn, discover, and make recommendations or predictions. The other software category is cognitive platforms, which facilitate the development of intelligent, advisory, and cognitively enabled applications. Industries will also invest in IT services to help with the development and implementation of their cognitive/AI systems and business services such as consulting and horizontal business process outsourcing related to these systems. The smallest category of technology spending will be the hardware (servers and storage) needed to support the systems.

On a geographic basis, the United States will deliver more than three quarters of all spending on cognitive/AI systems in 2018, led by the retail and banking industries. Western Europe will be the second largest region in 2018, led by retail, discrete manufacturing and banking. The strongest spending growth over the five-year forecast will be in Japan (73.5% CAGR) and Asia/Pacific (excluding Japan and China) (72.9% CAGR). China will also experience strong spending growth throughout the forecast (68.2% CAGR).

"The latest iteration of the Cognitive/AI Spending Guide is a roadmap for the journey of organizational digital transformation through the use of AI, deep learning, and machine learning," added Schubmehl. "Organizations should be evaluating and starting to use AI throughout their systems and the Cognitive/AI Spending Guide is an indispensable resource in that effort."

The Worldwide Semiannual Cognitive Artificial Intelligence Systems Spending Guide sizes spending for technologies that analyze, organize, access, and provide advisory services based on a range of unstructured information. The spending guide quantifies the cognitive computing opportunity by providing data for more than 20 use cases across 16 industries in eight regions. Data is also available for the related hardware, software, and services categories. Unlike any other research in the industry, the detailed segmentation and timely, global data is designed to help suppliers targeting the market to identify market opportunities and execute an effective strategy ■



Why Cryptocurrency Security Should Be On Everyone's Radar?

While attacks are more prevalent against Microsoft Windows, threats against Android devices are increasing as well

By Wias Issa

It's been easy for most people – even IT security teams – to avoid thinking about the security risks of cryptocurrency. Even as the price of bitcoin, ethereum and many of the "alt coins" comprising the cryptocurrency market skyrocketed towards the end of 2017, any security risks only affected the people holding cryptocurrency.

That is, until companies began to discover their servers — and even mobile devices — were being used by cyber thieves to mine cryptocurrency. Now, suddenly, cryptocurrency is bleeding into the world of corporate security teams in new and very real ways.

The way cryptocurrency affects consumer and corporate security is an evolving conversation that started several years ago. Here's a look at why it's more important now than ever.

Bitcoin Born: Underground Usage Grows

In many ways, cryptocurrency was a product of the 2008 banking crisis, conceptualized as a peer-to-peer value exchange system that could make people less reliant on banks. However, its anonymous nature meant that bitcoin was quickly adopted as a currency for criminals on the dark web.

Corporate IT teams and consumers alike need to be highly attuned to what's happening in their environments and ensure they're leveraging a combination of automated security tools with advanced threat protection and human-led inspection processes to ensure they don't become the victims of mining attacks

Cybercriminals began using bitcoin to send and receive payments for digital dossiers and credit card information, exploit kits and the many other cybercrime products and services available in the underground market.

Many security teams and consumers alike had their first introduction to cryptocurrency when ransomware began to run rampant in 2016. Often, victims were asked to pay their ransom in bitcoin, as this was largely untraceable by authorities and cut out much of the typical money laundering work.

In 2017, SonicWall researchers analyzed bitcoin data to find that transactions via ransomware-related wallet addresses dropped. This may partly be due to improved security efforts thwarting ransomware, and partly due to other cybercrime developments we'll discuss in a moment.

Normal People Get Involved: Cryptocurrency Wallets Targets for Cybercriminals

Before money began flowing into cryptocurrency, cybercriminals took the opportunity to attack several cryptocurrency exchanges. Many of the more famous exchange attacks predate 2017, including the Mt. Gox attack, in which users lost around USD 400 million and the DAO theft of about USD 50 million. Cybercriminals can't resist a hot market, so exchange attacks have become a staple of the cryptocurrency world. The largest successful attack happened in January 2018 when users of the Japanese cryptocurrency exchange Coincheck lost USD 530 million, according to officials.

The problem with losing money in a cryptocurrency exchange hack is that there is little or no recourse for the individual user. Cryptocurrency is anonymous and largely unregulated. Money in the cryptocurrency market is not insured in the way a bank account is, so when attackers walk away with millions, that's usually the end of the story.

However, in 2017, law enforcement arrested Russian Alexander Vinnik on more than 21 charges of money laundering, fraud and other financial crimes. He is believed to be responsible in some way for the Mt. Gox theft, since 530,000 of the bitcoin stolen in that attack ended up passing through wallets he controlled or was associated with. Of course, that's little comfort for Mt. Gox victims, who will remain unable to recover their funds.

Risk Expands: The Rise of Mining Hacks

The price of cryptocurrencies may not be what it was in December, but it's still a market with plenty of money to entice cybercriminals. In 2018, we expect to see a rise in attacks that quietly install cryptocurrency mining software on user devices and corporate servers.

This type of attack is only going to escalate this year, and we can expect mobile devices, desktops and corporate servers alike to be targets. Our recent analysis shows that, while such attacks are more prevalent against Microsoft Windows, threats against Android devices are increasing as well.

Focus on Reducing Your Risk

As with virtually any security risk, taking the right precautions can go a long way to keeping you safe.

If you hold cryptocurrency, don't leave large amounts on an exchange. Educate yourself on secure ways to store and transact with cryptocurrency, and do not take any risks you wouldn't want a bank taking with your money.

Corporate IT teams and consumers alike need to be highly attuned to what's happening in their environments and ensure they're leveraging a combination of automated security tools with advanced threat protection and human-led inspection processes to ensure they don't become the victims of mining attacks.

If you haven't begun to consider the threat of exchange and mining attacks in your personal or corporate IT security plan, the time has come to get serious about reducing cryptocurrency-related risks. The conversation around cryptocurrency will continue to evolve in the months to come, and if organizations don't stay tuned in and active, they're much more likely to become victims themselves ■

The author is Vice President and General Manager, Asia-Pacific & Japan, SonicWall

Cambridge Analytica Case: Look Beyond The Scam

While the scam may be the immediate news, the episode should also serve as a wake-up call for businesses which are yet to realize the capabilities of big data analytics

By Shyamanuja Das

The Indian media, like its counterpart in the West, has focused on the supposed 'scam' involving Cambridge Analytica (CA), the UK-based big data firm that helped in Donald Trump's victory through big data analytics.

The controversy started with a remark by its now-ousted CEO Alexander Nix, made to undercover Channel 4 News reporters about how elections can be influenced through what is very clearly unfair means, even while taking a public posture that the company does not cross the line of ethics. This came after New York Times and The Observer published how a UK-based company Global Science Research (GSR), hired by Cambridge Analytica, created an app and collected data from millions of Facebook users, in what Facebook claims to be 'in violation' of its policies.

Rest assured, we have a lot to see in the days to come. With GDPR kick-off date just about two months away, a lot of that debate may focus on data privacy with Facebook too as a target. Facebook CEO, Mark Zuckerberg, has been warned by authorities in the US and Europe for a possible testimony. Indian IT and communications minister, Ravi Shankar Prasad has also warned Facebook of stringent actions if any wrongdoing is discovered.

Role in Indian Elections

Prasad's warning comes after it emerged that Cambridge Analytica had been active in India too.

"CA was contracted to undertake an in-depth electorate analysis for the Bihar Assembly Election in 2010. The core challenge was to identify the floating/swing voters for each of the parties and to measure their levels electoral apathy, a result of the poor and unchanging condition of the state after 15 years of incum-

bent rule. In addition to the research phase, CA were tasked to organise the party base at the village level by creating a communication hierarchy to increase supporter motivation. Our client achieved a landslide victory, with over 90% of total seats targeted by CA being won," the company's website says.

The 2010 elections in Bihar was won by Nitish Kumar's Janata Dal (United) against Lalu Prasad Yadav's RJD, bettering their tally in the previous elections.

Interestingly, CA was established by its parent company, Strategic Communications Lab (SCL) in 2013. However, according to a report by the website thewire.in, SCL worked with a Ghaziabad-based company, Ovelene Business Intelligence (OBI), run by Amrish Tyagi, the son of senior JD(U) leader KC Tyagi.

"OBI is Cambridge Analytica's go-to company on the ground in the Indian subcontinent," says thewire.in report. It quotes Tyagi junior who explains that being partners, they can use each other's experience while making a pitch. This suggests that the work in 2010 Bihar elections was carried out by OBI.

What it means is that full five years before Prashant Kishor's 'famed' election strategy and execution for JD(U)-RJD's landslide in 2015 Bihar assembly elections, the Big Data game was very much there in India.

With India's—and specifically Bihar's—demographic reality, Facebook could have helped a little.

So, it is primarily data analytics that can be credited for this successful show.

I think that is something that is a takeaway from the entire episode. That Indian political parties were already doing this by 2010, full six years before Trump won using 'Big Data' in the US.

It is now well-known that prime minister Modi too relied on data analytics (interestingly, same Prashant Kishor) in his 2014 Lok Sabha elections. Maybe, he did that earlier in Gujarat elections too.

> With digital shifting the business thinking from inside-out to outside-in, it is an important aspect businesses may be missing out

In 2009, a strongman in a regional political party in Eastern India (who later fell out with his leader) used scientific data collection and juxtaposing that, with publicly available data, such as Census data and data from National Sample Survey Organization, to create successful election strategies for his party. The party severed its ties with one of the national parties and came to power on its own in the elections.

So, even in the muddy, free-for-all politics in India, political parties have started relying on data analytics, using both scientific data collection as well as making good use of publicly available data.

According to report by Moneycontrol.com, Cambridge Analytica itself had started focusing on the 2019 General Elections by being "in talks with a large opposition party in India" and had even made a presentation to the party in August. The report says it had "etched a data-driven strategy to target voters on social media, analyzing online user behaviour and connecting the dots across different citizen databases."

Where businesses lag

All this raises an obvious question. Does this mean political parties are ahead in the Big Data game?

In terms of usage of analytics tools, probably not. But one of the areas where political parties seem to have a clear lead is in using open data—or any publicly available data, for that matter.

There could be four major sources of data for a business:

1. Internally available data
2. New data collected through custom research
3. External data available publicly free or for a price and now
4. Social media data, which is updated in real time

Out of the four, businesses have been focused mostly on the first two while the fourth has been the Holy Grail. But most of them have ignored the third one—publicly available data, which can add immense value to the businesses if analyzed in conjunction with their internal or research data.

The social sector has been doing a lot of work using that data.

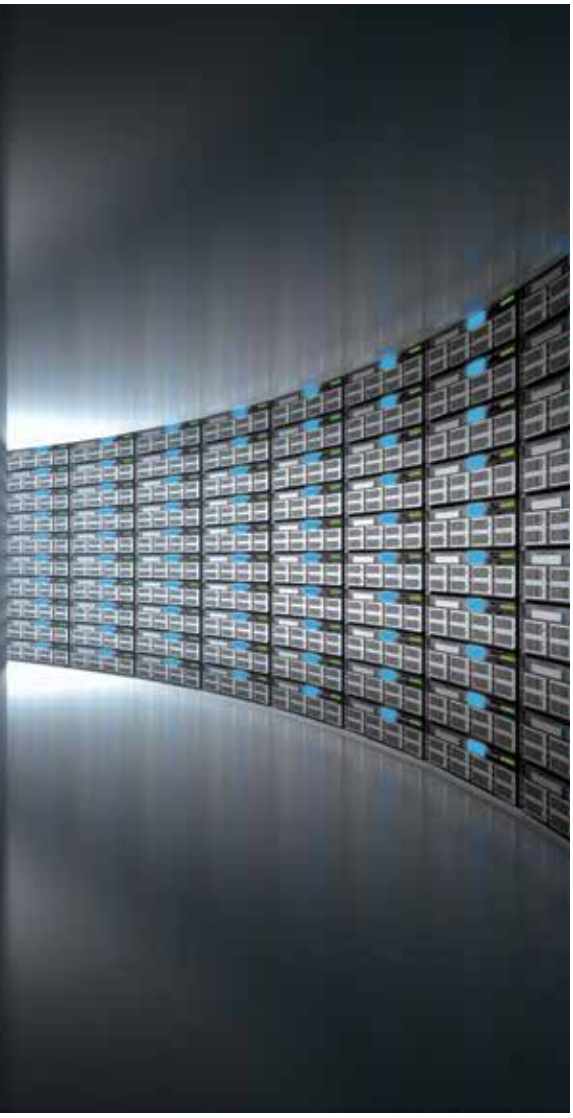
"Many businesses think unless they throw some big money and hire a big name to spend some time with, they cannot get any value," says a digital marketing executive and an open data enthusiast, rather bitterly.

The whole thing provides the businesses with an opportunity to open their eyes to the possibilities that the political parties have already sensed.

You do not have to steal data for that. You just have to think outside-in. Interestingly, the ability to do that has come as a strong pre-requisite for the digital leaders, in a research we have just completed on digital transformation in Indian companies.

You may make or get amused by a smart, sarcasm-laden Twitter comment and move ahead, but it is also not such a bad idea to pause a bit and focus on the possibilities ■

"CIOs need to choose the most compatible and secure datacenter solution"



Sanjay Motwani, Regional Director, Raritan Asia-Pacific shares his views on intelligent datacenters and parameters CIOs consider in choosing the right datacenter solution partner

By ITNEXT

Sanjay Motwani, Regional Director, Raritan Asia-Pacific shares his views on intelligent datacenters, parameters CIOs consider in choosing the right datacenter solution partner and how his company is positioned for the future in the datacenter space.

Here are the excerpts:

Q Can you elaborate a bit on the path traversed by intelligent datacenters?

A In 2007, Raritan was the first to add a user-programmable computer to a networked rack PDU to create a platform for smarter racks and intelligent datacenters. As a result, datacenter operators can now monitor energy, power capacity, temperature, humidity, and the status of PDUs, lines, circuit breakers and individual outlets—as well as power cycle IT equipment remotely.

In 2015, Raritan got acquired by Legrand taking over its power and KVM solutions. Its DCIM business was spun off into Sunbird Software.

Currently, Raritan is a renowned name in the KVM category and the technology leader in power management solutions with over 200 customers across its solutions in India. Its market-ready solutions in power and remote management facilitate datacenter managers to achieve higher productivity, more scalability and lower operating costs.

In 2004, Raritan started its India operations and has built a significant base of growing and satisfied customers over the years. Today, we have clients across sectors including BFSI, IT/ ITES, telecom, manufacturing, Government and PSUs.

Q Can you elaborate the concept of Edge datacenter? How is it going to help the CIOs in the enterprises?

A Trends like IoT or 4G will lead to the generation of massive volumes of data, while companies continually seek declining levels of latency. This data has to be managed, processed and stored in real time and closer to the point where it

"With the integrated portfolio and approach, our future road map includes deepening our existing engagements with large datacenter operations across the country in BFSI, Telecom, IT/ITES, Manufacturing and Government/PSU's"

— Sanjay Motwani, Regional Director, Raritan Asia-Pacific

is generated for efficiency. Key data, including data needed by other applications and people, will in some cases be made available at the 'near edge' in large datacenters where colocation and other metro datacenters are sited close to where the data is generated. Cloud heavyweights are rapidly building hyperscale datacenters with direct fiber links to leased colocation sites. This brings hyperscale cloud capacity closer to the edge – effectively functioning as 'near edge' datacenter capacity. Cloud providers will also utilize 'cloudlets' – distributed edge capacity for data caching or low-latency compute.

Once consumed or integrated, data will then typically be moved or streamed into large or hyperscale remote datacenters to be aggregated, analyzed (including through integration with other data and applications) and archived. These large facilities represent the 'core layer.'

By moving analytics to the edge, organizations or CIOs of enterprises will get immediate insights and results from IoT devices and sensors. CIOs will see benefits in terms of response time or latency. Shifting to edge also helps collocation service providers to offer better performance, more cost effectively.

Q In your view, what are the parameters CIO should evaluate in choosing the right datacenter solutions partner in their digital journey?

A Datacenters are rapidly evolving both in size and structure. The pace of growth will only accelerate further as 'data' becomes the currency for the digital transformation of companies and countries. CIOs therefore need a partner who will provide advanced solutions to the changing datacenter environment. The solutions offered should be modular, deployed quickly, scaled easily and operated efficiently. The criteria should not be whether the vendor can meet today's requirements but how fast, efficient and cost effective a partner they will be for tomorrow's datacenter requirements.

With increased complexity, the number of products and solutions deployed at the datacenter increases exponentially. Compatibility then becomes a key factor to consider when choosing a datacenter solution, keeping in mind not just today's requirements but new requirements along the way.

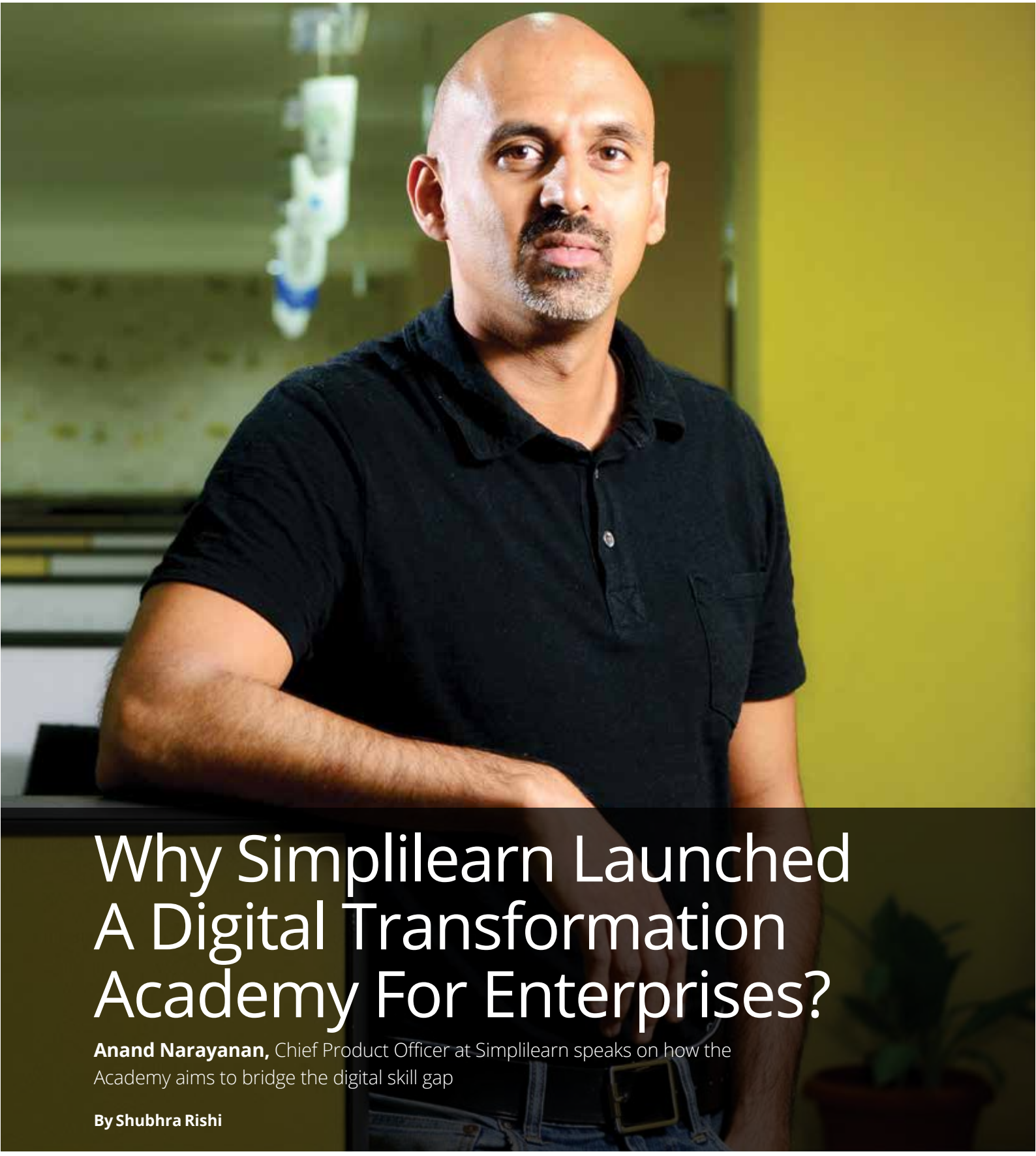
Finally, security of the data continues to be growing concern as the number of data users, access points, software and hardware in use increase. Organizations need to invest the most secure solutions, even if they come at a higher cost as the cost of a data breach is prohibitive.

Q Can you really future proof the datacenter investment? As a major technology company in this space, how are you positioned for the future?

A Post the acquisition by Legrand, we are now in a position to offer an integrated datacenter solution which includes leading domestic and international brands in UPS, racks, and structured cabling while Raritan continues to be the market leader in KVMs, power, iPDUs and environment monitoring segments. So our future roadmap will focus on integrating all our products and solutions and providing a one stop partner for our customers' datacenter requirements.

With the integrated portfolio and approach, our future road map includes deepening our existing engagements with large datacenter operations across the country in BFSI, Telecom, IT/ITES, Manufacturing and government/ PSU's. We will also be widening our brand footprint to reach the SMB segment across manufacturing, services, digital, education, healthcare, media and other industry sectors with the support of our partners.

We will continue to innovate and customize products and solutions based on a future-proofed architecture to handle today's and tomorrow's datacenter challenges ■



Why Simplilearn Launched A Digital Transformation Academy For Enterprises?

Anand Narayanan, Chief Product Officer at Simplilearn speaks on how the Academy aims to bridge the digital skill gap

By Shubhra Rishi

In the last few years, CIOs have been chanting the 'digital transformation' catchphrase as if it is a common cure for all enterprise IT worries. However, a lot of organizations have embarked on standalone digital initiatives and are slowly evolving their digital readiness. However, a frequent issue that companies face is the lack of available talent to lead these innovations. As a result, a lot of companies are looking at hiring outside skills for the duration of the initiative. Some are also working with startups or external vendors. What about enterprises/CIOs that are planning to upskill their existing workforce on digital skills?

A quick Google search displays several courses offered by premiere institutions such as Indian School of Business (ISB), and online courses by platforms, such as Udemy, Coursera, edX among others. Simplilearn, a professional online certification provider, recently launched Digital Transformation Academy – a complete suite of courses tailored for enterprise needs.

We spoke to Anand Narayanan, Chief Product Officer at Simplilearn, to find out how the Academy aims to bridge the digital skill gap.

> "CIOs are realizing that there is a significant technology shift happening in the industry with the mainstream use of digital technologies and this is clear from the way their training budgets are being allocated"
>
> - **Anand Narayanan**, Chief Product Officer at Simplilearn

Q Digital Transformation is a very broad concept. How do you define it at Simplilearn?

A We believe that, to successfully drive Digital Transformation, any organization needs to pay attention to three foundational aspects: People, Process, and Technology. The people aspect includes the process of transforming the mindset of an organization and creating an innovation driven culture from the grounds up. Process involves the ability to be "agile" and always follow "devops" principles. And finally technology allows an organization to change the way business is performed. Digital transformation isn't just about technology but is also about the people that drive it and the processes that foster innovations.

Q Can you talk about the skill gap issue in enterprise IT?

A Digital transformation is already disrupting traditional technologies, replacing them with digital domains, such as AI & Machine Learning, Analytics, Cloud, and Robotic Process Automation. It is also clear that these skills are not easily acquired due to their rapid evolution.

As an example, industry estimates show that there is a need for X Machine learning engineers, with the number of filled positions only Y. To remain competitive and efficient, organizations have tried hiring for these skills, but the talent pool remains small. This leads to a skill gap that can only be overcome with a strong upskilling program.

Q We conducted a survey of IT Managers recently and found that only less than half of them have completed any kind of certification in the last two years. Every three out of four of the respondents said they have done some kind of certification in the last five years. Why do you think CIOs/IT managers will be interested in taking up what you have to offer?

A Enterprises, more than ever, are measuring the ROI of their employees and realizing that they are falling behind on key skills in the digital domain. Online learning does not drive user engagement and the completion rates are abysmal as a result. The Simplilearn learning approach drives user engagement and skill achievement through a high-engagement, outcome centric model. Online self learning content, skills assessments, live classes with industry grade faculty, teaching assistants to intervene when required and hands on projects, have helped us to deliver an industry high 72% completion rate on our curriculum. Being able to achieve the learning outcomes and truly transform their organization is what

makes our offer exciting to these CIOs/IT managers.

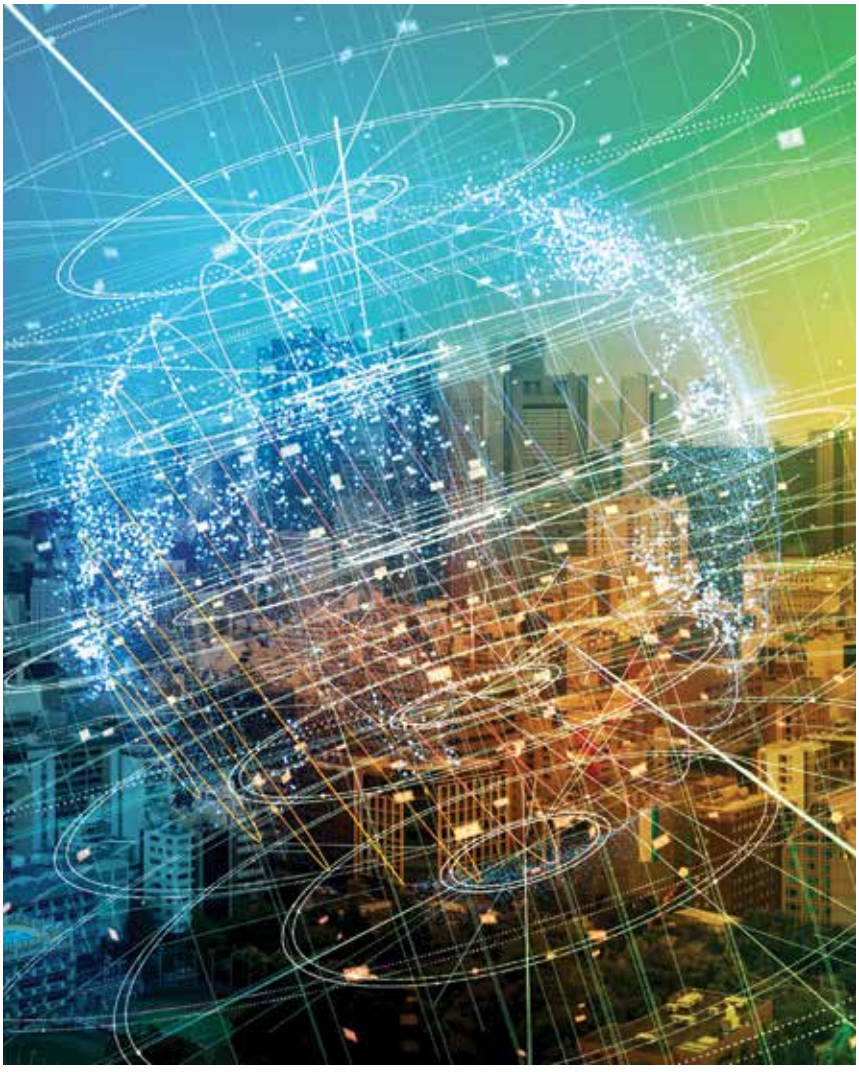
Q Another survey finding that we encountered was that 28% of IT Managers said they would go for learning new technologies; however, leadership skills still topped the choice list. Clearly leadership skills are a CIO's top priority and they would rather spend dollars on hiring temporary skills. Then why would CIOs reskill Wat all or do you feel differently about this?

A In recent focus groups and discussions that Simplilearn has had with CIOs and L&D heads, it was clear that while the target group thought that leadership skills were important, a majority of their budgets were going towards technology training. IT Managers and CIOs are realizing that there is a significant technology shift happening in the industry with the mainstream use of digital technologies and this is clear from the way their training budgets are being allocated.

While there has been intermittent use of a transient workforce, this approach has not delivered a culturally aligned outcome for these corporations. This transient workforce solves for the technology aspect, but it fails to deliver on the people and process aspects due to poor alignment of outcomes. It has become an imperative for corporations to upskill their employees or risk being left behind as a result.

Q What's the vision and mission of the Simplilearn Digital Transformation Academy for enterprises?

A The Simplilearn Digital Transformation Academy is our flagship initiative to enable enterprises become digital ready. We are partnering with organizations to equip them with the skills needed to survive the digital era. The Academy has a suite of training programs that help organizations become competent in digital technologies. The program covers all knowledge aspects of the people, processes and technology framework and allows any organization to quickly move up the digital transformation capability ladder.



Q What is the broad breakup of the course module?

A The Simplilearn Digital Transformation Academy covers varied topics across the people, process and technology aspects. On the people side, the academy provides training around design thinking, and UX principles which can lead to a more innovative, customer centric approach within an organization.

On the process side, the academy covers core topics such as Agile and DevOps which allow an organization to run lean and fast. And on the technology side core digital disciplines are covered such as AI and machine learning, robotic process automation, big data, data analytics, digital marketing, and cloud computing.

Our outcome centric curriculum is a blend of online self-learning and live instructor led classroom, allowing the learner to learn from anywhere. The courses are designed for three levels of training - Practitioner, Consultant, and CXO, and are based on the depth of knowledge and digital expertise required for various roles. Additionally the academy provides the capability to customize the curriculum for specific verticals ■

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

Double Scoop

Two times the revelation

Anand Rajhans

Head–Technical Integration & Shared Platform Services, Syngenta

A PERSON WHOM I IDOLIZE IN LIFE

Gautam Buddha

MY FAVORITE CUISINE

Puran Poli

MY FAVORITE GETAWAY

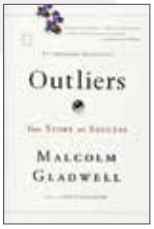
Keukenhof Gardens in the Netherlands

A TECH WHICH WILL DOMINATE IN 2018

Robotics powered by AI

A NON-TECH BOOK WHICH I'M CURRENTLY READING

Outliers by Malcolm Gladwell



MY PEER IN THE IT COMMUNITY

Jeevan Chaukar

Head – ITSM, Shiksha Infotech

MY FAVORITE WRITERS

Michael Crichton and Sir Arthur Conan Doyle

TECH SYSTEMS I'M CURRENTLY WORKING ON

BMC Remedy ITSM and ServiceNow ITSM

A SONG WHICH I LIKE THE MOST

Ruk Jana Nahin Tu Kahin Haar Ke by Kishore Kumar

MY IDEAL PAST-TIME

Motor-cycle riding

APPS WHICH I USE THE MOST

Paytm, Amazon, Uber

Companies worth
5,000 crore of **security budget** will come under one roof to discuss the **future of IT security**
on

25th - 26th May 2018

10TH ANNUAL CSO SUMMIT
WHAT'S NEXT?
&
nextCSO AWARDS
THE SEARCH FOR INDIA's FUTURE CSOs

25th-26th May 2018 | Crowne Plaza, Greater Noida, UP

#NEXTCSO

Presenting Partner: Google Cloud
Associate Partner: eScan Enterprise Security
Organised by: CSOFORUM
A Brand of: 9.9 GROUP

COME JOIN THE DISCUSSION