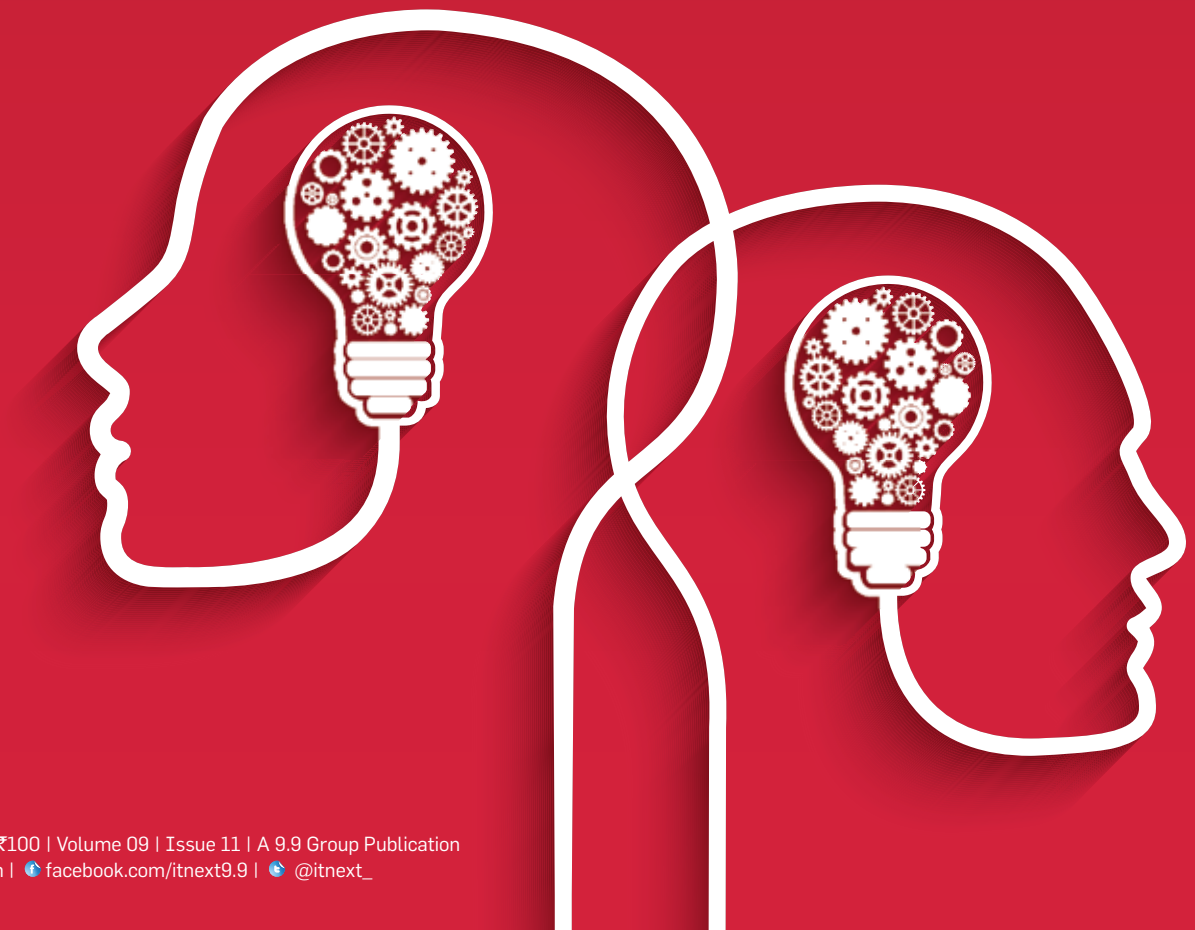
Opinion | Pg 22
CIOs Can Harness Dark Data To Boost Innovation

Insight | Pg 24
Rethink Security With Zero Trust

ITNEXT
FOR THE NEXT GENERATION OF CIOs

Revisiting CEO-CIO Relationship

As technology starts influencing business models, the scope for CIO's value addition to business grows manifold. That opens avenues for more meaningful CIO-CEO relationships



April 2019 | ₹100 | Volume 09 | Issue 11 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

Why IT Managers Should Become Role Makers?

"The newer importance of technology in business is in the areas of strategy and business model. There, the problems—more often than not—are not well defined. Either, the canvas is blank or is too confusing."

Shyamanuja Das

In the last twenty years, role of technology in business has changed dramatically. Today, technology is not just impacting products and processes, it is impacting strategy as well. Business models are dictated by technology.

As an IT leader, can you vouch that the importance of CIO has grown proportionately? Far from it; in fact, we are seeing question marks about the utility of CIO position.

Many IT leaders are still in denial mode. They point to some CIOs being given important corporate roles, such as HR, supply chain, administration, etc. in some large enterprises.

If some CIOs are given newer non-IT responsibilities, it is because of their capabilities as individuals. If anything, it proves that these capable people have nothing much to do within IT. The companies have optimally utilized their talent and capability by giving them other responsibilities.

But what explains this anomaly—while role of technology has grown manifold, the CIO's importance has not?

I think it is the way the CIOs themselves—and hence others in organization—have seen their roles. While many CIOs today understand business, they have remained at an arm's length from business decisions. Once the business decisions are taken, some of them are excellent at providing a technology solution. But when the canvas is blank, they do not know what to do.

The newer importance of technology in business is in the areas of strategy and business model. There, the problems—more often than not—are not well defined. Either, the canvas is blank or is too confusing. Since technology is an integral part today, it has to be interwoven to the business decision itself at that stage. It is not a subsequent decision.

Traditional IT managers are not used to such expectations.

This also explains why so many start-ups do not have full-fledged CIOs. One of the founders or top executives, often called CTO, technology head or product head, drives strategic technology and products and someone reporting to him/her looks after enterprise IT.

Most large organizations are trying to move towards that model—which means lesser and lesser role for traditional IT managers, even though their importance is not diminishing in any way. As more and more parts of business gets digitized, there would be bigger need for management and support of IT infrastructure. That will continue to be managed by IT managers.

If IT managers want to lead transformation and take more strategic roles—they just need one change. They must be role makers, not role takers■

APRIL 2019
VOLUME 09 | ISSUE 11

Content

Revisiting CEO-CIO Relationship

The current technological advancements in the digital era provide excellent opportunities for CIOs to actively contribute to shaping business strategies and growth while striking a strategic partnership with the CEO

COVER STORY | PAGE 10

Cover Design:
CHARU DWIVEDI

ADVERTISER INDEX

TSL	BC

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

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

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

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

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

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

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

OFFICE ADDRESS

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

Editor: Vikas Gupta

99 GROUP

EXTRA Curricular

Not just a passion, but a teacher for life

The King of Waters

NEXT100 Winner 2011 **Prashant Singh**, Associate Director, KPMG India, shares his immense passion for swimming besides listening to music and reading books...

"Swimming is normal for me. I'm relaxed. I'm comfortable, and I know my surroundings. It's my home." **– Michael Phelps**

"As long as I'm enjoying swimming, I will keep swimming." **– Cate Campbell**

"Swimming is my passion and something that I love." **- Natalie du Toit**

"I won't give up swimming, even if it kills me. I love the rhythm of it." **– Arturo O' Farrill**

I started swimming when I was 12 years old. A Punjabi by birth, growing up in the warm climate of Hyderabad, I was always trying to escape the heat and swimming provided a perfect reprieve.

My earliest memories of swimming are of my mother and her brother swimming in the ocean in Vishakapatnam where my mother's parents were stationed. While I was resigned to wallow in the sandy waves breaking over my back and tasting the salt and grit in my mouth with every wave, I would watch with awe as my mother would effortlessly swim in the deep ocean where you could ride the waves and float on your back when you got tired – I wanted to do that.

Swimming did not come naturally to me and

Prashant Singh

Snapshot

Prashant Singh is a NEXT100 Winner of 2011. He is Associate Director at KPMG India. Earlier, he was with Sistema Shyam Teleservices. He completed his MBA and PG Diploma from Indian School of Business and Bachelor of Engineering from Cochin University of Science and Technology.

initially it took a lot of effort by my coach and constant prodding by my parents to take up this activity. In fact I remember clawing at the grass next to the swimming pool while being dragged and plunged into the pool by my coach!

After the initial learning pangs though, I really took to water as a fish and enjoyed the activity. In the pool, I have taken part in friendly races, played the regular games (toss the coin/soda cap) and these days devote a large part of my time to teaching my kids. However, I enjoy swimming in the ocean most – the vast openness provides me with both humility and confidence of being in control. I've swum many times in the Arabian Sea on the beaches of Goa and enjoy riding the waves and swimming against the tide – but my most memorable swim in the sea was along the beach of Kovalam (Kerala) where my brother and I were swimming behind the break-line in the afternoon tide. In the high tide, the waves coming in were more than 6 feet high before breaking and every time we rode a wave, we would be lifted up higher than the beach umbrellas on the beach, providing us with a panoramic view of the beach from the sea. It was a view few on that beach would get to see and it was worth burning our backs staying out at sea for more than an hour on that sunny afternoon.

I love swimming as it provides multiple contrasting experiences simultaneously:

Improving the quality of life in every stroke

- It can be both exhilarating (when diving into a cool pool early in the morning) and soothing (float on the water with your eyes closed – it's better than listening to music on a headphone with active noise cancellation!)
- Grueling (5 laps in 3 minutes) and relaxing (a lazy lap with minimal splashing)
- Exercise-oriented (try regular warm-up exercises when standing in the water) and fun-oriented (spending quality time with my kids and helping them get comfortable with the water)

Swimming teaches many valuable management lessons directly applicable to everyday work:

- Breathing techniques teach us that discipline, control and monitoring are key to mastering the basics
- Different swimming techniques teach us that there is always more than one solution to a problem but in each solution, there is an approach that is most efficient – the art is in knowing which technique to apply and what is the best approach to take to tackle any issue
- Practice and reflection, that is feedback is required to constantly get better – continuous improvement

However, for me, swimming is more than multiple experiences and lessons/reflections. It provides me with what I need no matter in what state of mind I am in. I am not an award winning swimmer, but I am definitely a passionate one.

I also love reading books, listening to music (preferably 80s rock) when I find the time and am an amateur foodie. But none of my other hobbies can give me the fulfillment of spending an hour in the pool!■

As told to Dipanjan Mitra, Team ITNEXT

CIOs Need To Leverage The Power Of Innovation

Vineet Bhardwaj, Head – IT, Godrej Properties believes that IT forms the backbone of business and CIOs and IT leaders have an important role to play in driving business for the company

By Sohini Bagchi

Being the senior executive responsible for all the technology, running a company is not an easy task. Today's CIOs often have to wear many hats to get the job done, stay competitive and lead more successfully. **Vineet Bhardwaj, Head – IT, Godrej Properties**, a Chartered Accountant with a passion for technology, has had the opportunity to work in diverse companies and in various IT domains. He believes that IT forms the backbone of business and CIOs and IT leaders have an important role to play in driving business for the company. In a recent interaction with CIO&Leader, Bhardwaj speaks about his career journey, changing role of CIOs, his tryst with emerging technologies and also offers his pearls of wisdom to budding CIOs in the industry.

Q In India, a predominant majority of CIOs are career tech professionals. You are a CA. What made you switch to tech?

A As a Chartered Accountant, I started my career in finance and accounts department of one of the Navratna PSUs, however; soon I realized my love for technology and started looking at options internally to move into technology role. I got an opportunity when my organization went in for SAP implementation and based on my interest and passion, I was considered for being part of the core team for the said project. From there on, my passion for technology has only grown leaps and bounds and eventually became a technocrat. It has always fascinated me, how technology can impact and change the way businesses function. I love the freedom that my role allows me in assessing new technologies and examine them from the perspective of business challenges they solve as well as in exploring and optimizing them for our specific industry and organization. Organizations, over the years, are looking at leveraging technology, not only to enhance productivity and efficiency but also to make build competitive value proposition and create differentiation.

Q What are your key tech priorities in the next one year?

A In our endeavor to become a future-ready organization, we are leveraging technology as a foundation across various business processes, all in accordance with business dynamics. With us continually learning, evolving and leaping forward to keep pace with the rapid growth in technology, individual departments within GPL, themselves are becoming as agile and adaptive as the larger company. We are very keen to utilize apps to improve our business processes and to up the accessibility for our customers and employees. Just as in various other industries, Artificial Intelligence and Machine Learning are bound to be the next big thing in real estate. Besides, 3D printing technology may also become another major factor in shaping the growth of the real estate industry.

Q As a CIO what was the toughest decision you made?

A Making the decision between in-sourcing and outsourcing models – especially with IT services, because the technology is ever evolving, becomes obsolete quickly and consequently, the skill set associated with it changes as well. In order to have the right balance, we decided to have an internal team that is not just purely technical but holds more business and process-centric capabilities that are more of a techno-functional nature. On the other side, we choose to outsource work which requires certain specialized skills, either on a project basis or on a resource augmentation basis. This helps us to have the best of both worlds by having strong domain expertise in-house and agility to adapt to new technologies quickly.

> "The role of a CIO is moving in the direction of higher process automation which will exist in alignment with human tactical intervention on time-saving and improving productivity"

Q Where do you see the CIO role heading in the future?

A Businesses need their CIOs to be real partners in dealing with complexities and dynamism of business. The role of a CIO is moving in the direction of higher process automation which will exist in alignment with human tactical intervention on time-saving and improving productivity while maintaining great quality. In an increasingly technology-centric business environment with constant change in demands from the business, CIOs must find key game-changers in innovation and process improvement that genuinely impact the bottom line. Over time, the CIO's role has changed from that of simply a business support function to a business enabler and ultimately to a business driver. I visualize the CIO's role evolving even further into that of a business transformer, constantly building path-breaking innovations. Ultimately the CIO will stand in the position of an indispensable master strategist, thus driving the entire business system.

Q What are the new business challenges your company is facing this year?

A Real estate has seen constant change over recent years. With RERA, GST and constant policy changes from the government, business processes have gone through various changes within the short span of time. We are still on the trajectory of a learning curve with customer challenges, pricing and new needs. Taking this as another opportunity to grow, we are also bracing ourselves for the challenges.

Q How do you think new technologies like AI, IoT, Blockchain technology and chatbot can play a key role in accelerating innovation in the real estate industry?

A As part of GPLs 'Win for Employee' and 'Win for Customer' agenda, we have recently launched 'Infobot'. Under the aegis of the functional academies at GPL, we have leveraged Artificial Intelligence (AI) through our Real Estate (RE) Infobot.

"IT departments are drivers powering any business today. They need to involve themselves in all aspects of the business and align with other functions. Not just in implementing and executing ..."

Infobot helps employees from non-RE backgrounds (51%) to understand RE terminologies better. Employees can ask questions on anything RE-related and they will receive an immediate response. It answers over 300 potential queries that a new joinee could have regarding RE concepts. We have also ensured continuous & exemplary engagement with customers to deliver assured delight. Both the platforms possess a user-friendly interface, making them easy to use. Our customer bot is almost ready with all the important implementation. We have also set up smart homes which are an IoT based module which is also integrated with Amazon Smart Speakers. With regards to Blockchain, there's still a long way to go, and we haven't found any relevant case study to implement.

Q Please highlight some of your technology initiatives in recent years.

A One major initiative we have been driving over two years is the creation of "Unified Information Architecture". It was extremely satisfying the day our top management began using system generated reports and dashboards for periodic reviews and decision making was an important win according to me. While we had been working on building the information warehouse and the data analytics tools for a while, we were not achieving the toehold we were aiming at or the buy-in from the top management who was still leaning towards using Excel files and PowerPoint slides rather than a system generated report. Apart from this, we have started implementing smart home technology solutions and Alexa enabled homes. Providing customers and employees the AI experience is one important priority for us this year.

Q One thing that CIOs should take as a mantra...

A IT should take more part in the business decision-making process and not be confined to only the servicing & transactional mode. Rather, IT should aspire to lead the game as an integral part of the business. IT should solve challenges strategically and achieve a strong footing with every change in the organization as enablers. It's not easy but if IT teams start investing more effort in understanding business issues even before the business teams raise the problem; the tact of being predictive and not just agile will gradually develop. To stay ahead in the race, IT teams need to leverage the power of innovation and analytical thinking to ultimately counter the complex issues by building on the basics. IT departments, in reality, are drivers powering any business today. They need to involve themselves in all aspects of the business and align with other functions. Not just in implementing and executing but also in planning and strategizing.

Q After a busy working day, how do you unwind?

A Other than IT, I have an interest in music and would like to learn to play drums sometime in this life (smiles). I believe in maintaining a work-life balance and try to spend quality time with my wife Pooja and two kids, Aryan and Aishani■

WHO CAN APPLY?

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

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

WHY APPLY?

By participating in the NEXT100 process you get:

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

HOW TO APPLY?

To get started with the NEXT100 application process:

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

APPLICATION OPEN
20TH MAY

APPLICATION CLOSE
1ST JULY

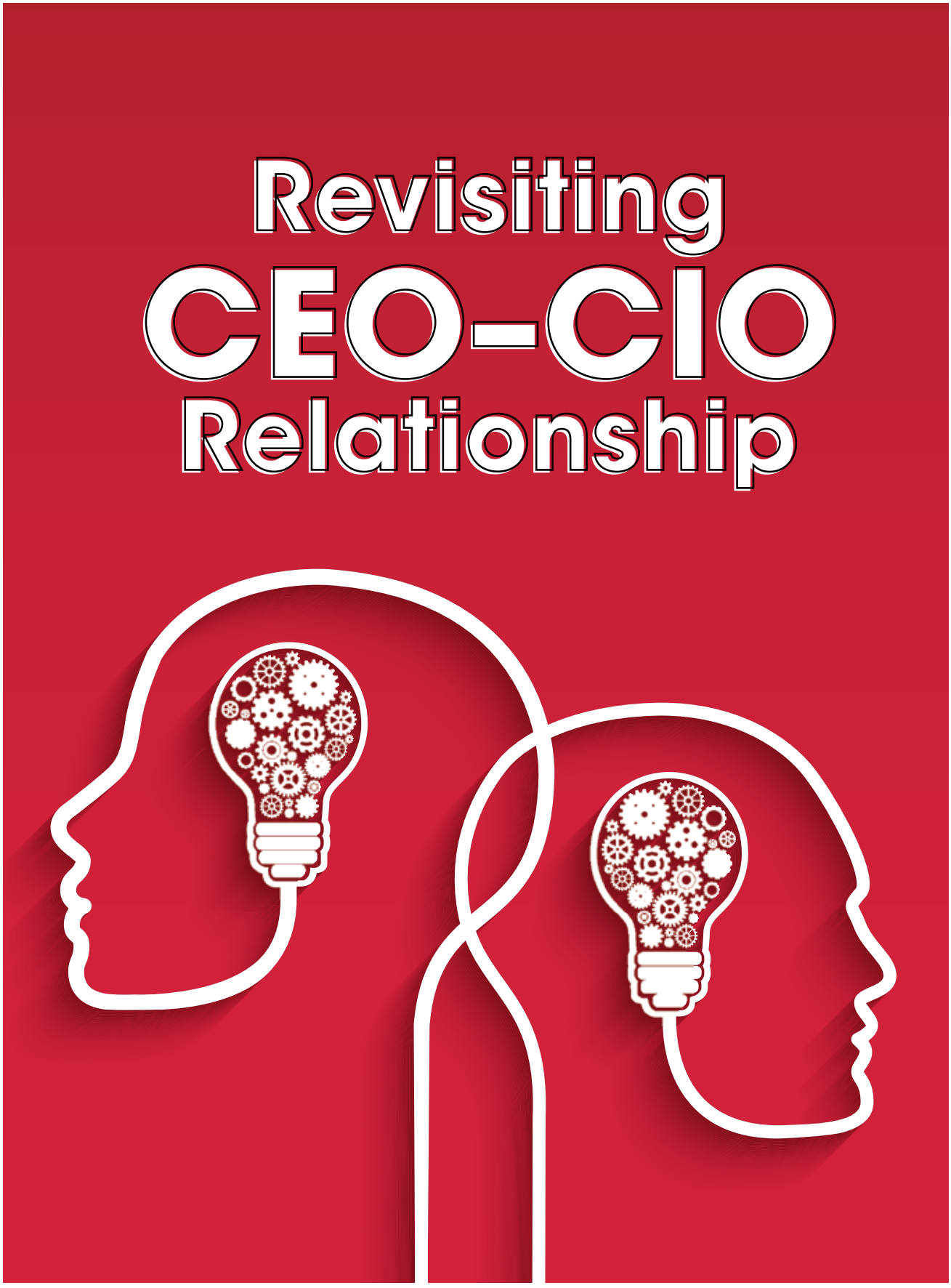
APPLY NOW
For details, please log on to
next100.itnext.in

INDIA's FUTURE CIOs
NEXT 100
2019

10 years
2010-2019

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

Revisiting CEO-CIO Relationship



The current technological advancements in the digital era provide excellent opportunities for CIOs to actively contribute to shaping business strategies and growth while striking a strategic partnership with the CEO

By Sohini Bagchi

Traditionally, CIOs, who usually—and in India, predominantly—have come from a technology background, have found it challenging to effectively communicate with the CEOs, who generally come from a business background, typically sales or operations. Nor have the CEOs understood the technology lingo.

Things have changed for sure.

One, digital technologies have now touched multiple aspects of a business. So, a CEO cannot remain at a distance.

Two, there is, in general, a better awareness and sensitivity around new technologies. All tech things are not necessarily learnt through the CIO.

Three, technology's impact on business is not just in terms of breadth but also in terms of depth. "Applying technology to business needs has been done since ever..., but what is happening today is – you can impact all the three layers, strategy, product and processes today which was not possible earlier," says Sarajit Jha, Chief, Digital Value Acceleration at Tata Steel.

So, today the imperative, opportunity and scope for CIO-CEO effective collaboration are far more. Well, that is the beginning of a journey to the boardroom for CIOs.

Unfortunately, the ground reality seems to be a bit disappointing. Even today, most CIOs are comfortable with the proposal-approval model, rather than inviting their CEOs to participate in the IT decision-making process. "This non-engaging conversation with the CEO causes disengagement and is at the center of the many challenges that CIOs face," comments Leigh McMullen, research VP at Gartner.

He believes that this can lead CEOs to view the IT department as a service provider, rather than as a strategic business partner, which in turn, can lead to reduced IT budget and a lack of CIO involvement in the making of decisions that affect business outcomes.

Communication is the key

According to a 2018 Gartner research, CEOs continue to rank IT as an important strategic asset and as a means through which they can innovate. "While CIOs are trying to influence future investment choices or increase IT's credibility and business value, having an engaging conversation with their CEO is critical to being viewed as their CEO's 'close confidantes'," says McMullen, adding that this would also mean that the conversation the CIO has with the CEO should include how to improve profit margin and about gaining competitive advantage.

Digitalization is giving CIOs the opportunity to change their role from approval seeker to a contributor with a seat at the strategy table, believes, Kumar Parakala, an industry veteran who worked as a CIO with public and private sector organizations and is currently the Co-founder and Managing Director of digital firm, Technova.

"With digital disruption having placed technology at the heart of most business discussions, by exploiting the digital changes that lie ahead, CIOs can have a real influence and can be regarded by CEOs as an important strategic business confidant and partner," he says.

Agrees,Vishal Anand Gupta, Head – IT Applications at Religare Health Insurance, who emphasizes that CIOs should have a thorough understanding of business in order to expand his role beyond the realms of IT.

For instance, in an organization where the CEO is looking to expand his business in newer markets, the CIO may not be directly involved with the market expansion plans; rather he can influence the CEO on how the organization can leverage technologies to set them apart from their competitors while managing cost or risk exposure, among other things.

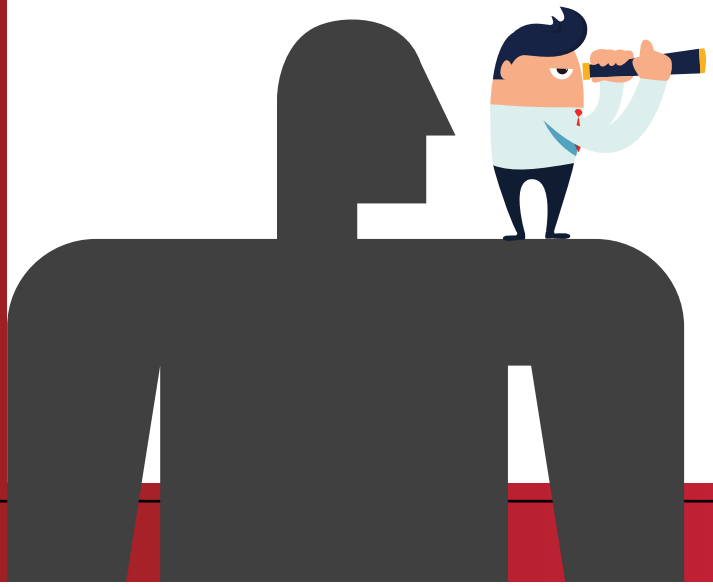
"The CIO needs to understand the company's business needs as well as the technologies being used, and accordingly, collaborates with CEO and others in the C-suite to understand its internal workings and needs," Gupta states.

But Parakala believes CIOs are at a crossroads in defining their role. While CIOs recognize there is a unique opportunity to leverage new and emerging digital technologies to enhance business growth, they also face several challenges – one being underinvestment in IT, which he sees as the primary barrier to a successful CEO-CIO partnership, as business leaders treat IT as a business commodity rather than as a business enabler.

Other factors, such as outdated legacy infrastructure, heavy reliance on IT vendors, poor understanding of technological benefits and how they can contribute to business growth as well as little CIO involvement in strategic business discussions and decisions often prevent CIOs from assisting their CEOs with business growth objectives.

In organizations that recognize several barriers and works towards it, CIOs can work closely with CEOs in shaping business strategies and growth.

> "The CIO needs to understand the company's business needs as well as the technologies being used, and accordingly, collaborate with CEO and others in the C-suite to understand its internal workings and needs"
>
> **Vishal Anand Gupta,** Head - IT Applications, Religare Health Insurance



Support from CEO and Board

While much has changed from the days when CIOs fought to have a place at C-level business table with cyber-security and digital transformation becoming a mandate, CIOs still believe boards should be more prepared to help and recognize the need for digital and a faster pace of business. In reality however, directors and CEOs don't always know what kind of business discourses they should have with the CIOs.

"Boards should guarantee the future health of the organization, magnify the change and think on a high level about the impact on the business. Disruption is after all driven by people and organizations. Boards ensure that the transition to digital is done properly, by creating digital risk profiles of the organization. And by showing management how they can develop a growth strategy using digital to increase the company's potential value creation," says Dr. Makarand Sawant, Senior General Manager - IT, Deepak

"It is mandatory for Boards to know what a company's digital strategy program is and what change it brings to the organization. Every board member should be aware of the impact digital transformation has on the company's business,"

Dr. Makarand Sawant, Senior General Manager - IT, Deepak Fertilisers And Petrochemicals Corporation Ltd. (DFPCL)

"Applying technology to business needs has been done since ever…but what is happening today is – you can impact all the three layers, strategy, product and processes today which was not possible earlier"

Sarajit Jha, Chief - Digital Value Acceleration, Tata Steel

Fertilisers And Petrochemicals Corporation Ltd. (DFPCL).

According to Sawant, it is mandatory for Boards to know what a company's digital strategy program is and what change it brings to the organization. "Every board member should be aware of the impact digital transformation has on the company's business," he states.

While CIOs are striving to connect with their CEO and boards in many firms, it may take a few more years for the CEO-CIO partnership to reach the heights of maturity. Studies show that CIOs are the youngest members of the C-suite. According to a 2017 study from advisory firm, Korn Ferry, CIOs are the youngest in the C-suite with the average CIO approximately 51 years old. CIOs also have a relatively short average tenure of 4.3 years. In contrast, CEOs are the oldest and longest-tenured members of the C-suite. Among all industries, the average CEO age is 58. In contrast, the average age of other C-suite leaders analyzed is 54. The average tenure is 5.3 years.

Also when one discusses digital transformation or even something as vital as succession plan, a question that comes up is who among the C-suite members can take up the digital leadership role. While some believe the obvious choice would be the CIO, since the discussion moves on to shaping the firm's digital strategy and he has the mastery over digital technology than the rest, a Harvard Business Review Analytic Services survey sponsored by Red Hat revealed most CEOs do not think their CIO is up to the task. This indicates that digital goes beyond 'mere technology practice' in the firm.

So, how can CIOs contribute to business growth agendas? Here are just a few logical ways CIOs can help their CEOs, states Parakala:

- Understanding new technologies and digital business strategies
- Engaging middle and senior managers to co-create innovative solutions in partnership with vendors
- Introducing collaborative tools and self-service portals to reduce human capital costs
- Educating Boards, CEOs and senior executives about disruptive trends and opportunities
- Actively engaging with vendors, industry bodies, experts and thought leaders to understand strategic trends in the industry to leverage innovative opportunities

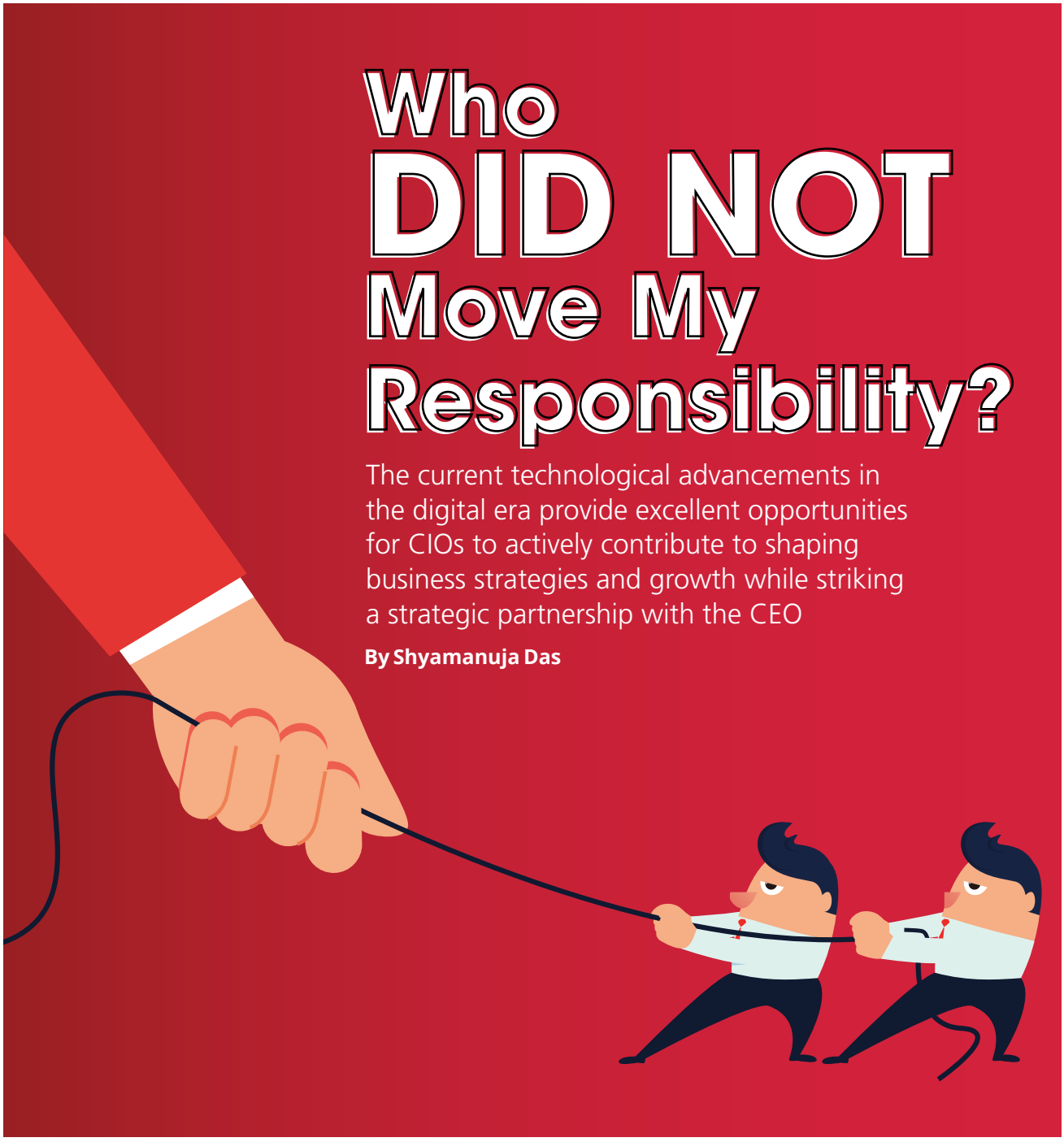
In the current scenario, CIOs can use technical expertise to "keep the lights on" while simultaneously using creative skills to facilitate the innovative use of new technologies for growth and customer engagement. CIOs need to embrace this dual role with importance emphasized on strategic business matters.

Needless to say then, despite all challenges, the current technological advancements in the digital era provide excellent opportunities for CIOs to actively contribute to shaping business strategies and growth while striking a strategic partnership with the CEO■

Who DID NOT Move My Responsibility?

The current technological advancements in the digital era provide excellent opportunities for CIOs to actively contribute to shaping business strategies and growth while striking a strategic partnership with the CEO

By Shyamanuja Das



Who is best suited to drive digital transformation? Not long back, this was a big debate between the Chief Marketing Officers (CMOs) and Chief Information Officers (CIOs). While the CMOs believed—at least that is what they said—as the people who understand the mind of the end customer, they were the best people to drive 'customer-centric' transformation, CIOs retorted—where would you be without technology that is increasingly impacting all aspects of the business; marketing is just one function, after all.

Both had their points. But finally, the debate seems to have been settled in favor of the core business guys. The Chief Digital Officer (CDO) positions in large companies have all been taken up by people with core business background, who have managed SBUs, run different parts of business, understand internal organizational dynamics well. According to an August 2018 study by CIO&Leader,

there were 49 Chief Digital Officers in large (excluding media/media-related services) companies in India. As many as 24 of them came from core business background. Only 15 came from technology and seven from marketing background.

[The consolation for CIOs is that they have won against the arch rivals, CMOs in this one-upmanship game. My rounds of discussion with other CXOs have convinced me that the CIOs' victory is—at least partially—a result of the comparatively higher level of trust that they enjoy as compared to CMOs with Chief Financial Officers, in some cases their immediate bosses. But that is another story.]

The point I am trying to make here is that the larger transformation role is increasingly being taken up by core business people. In hindsight, it looks fairly logical.

Does that mean the fear about CIOs' role becoming redundant—something that some analysts and writers have been discussing for last few years—is coming true?

Far from that.

Last year when I was doing a research on digital transformation in manufacturing sector, I spoke to quite a few senior 'transformers'—the Chief Digital Officers, the Head of Transformation, Chief Strategy Officers, etc. who were leading the transformation in their respective organizations.

Not even one of them told me that CIOs job was unimportant, let alone being redundant. Most of them talked quite respectfully of CIOs.

But the good news ends there.

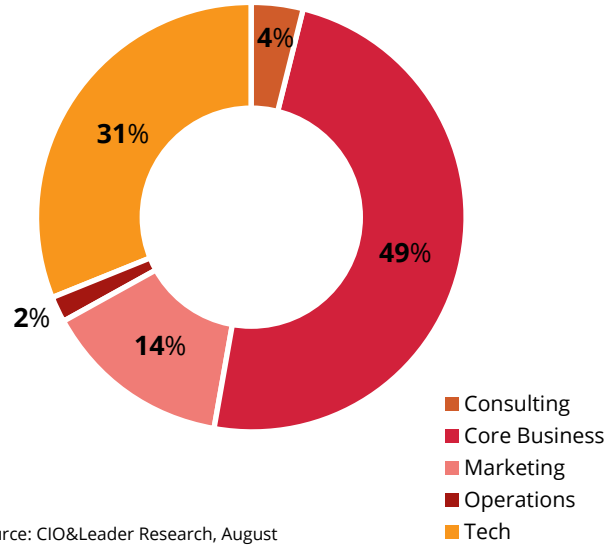
They justified the CIO's importance by arguing that as companies go more and more digital, the IT infrastructure to support that kind of digitalization—whether within the company or rented from a service provider—would be bigger and bigger. Managing that would be more and more important. Who would do that, if not the CIOs?

In other words, while they had tremendous respect for CIOs and justification for their utility, they had a completely different expectation from the CIO as compared to what the CIOs themselves believed, which is driving transformation.

Here, what I would like to remind you again is that I was talking to largely manufacturing companies, in some cases, diversified ones. But they were probably the most mature among manufacturing companies.

While the business people had tremendous respect for CIOs and justification for their utility, they have a completely different expectation from them as compared to what the CIOs themselves believe – which is driving transformation

Background of Chief Digital Officers



Source: CIO&Leader Research, August

Is technology becoming too big to leave it to the technologists?

This shows for new generation business leaders—who do not have a baggage of the past or any prejudices—the CIOs are excellent managers of technology infrastructure. They are the guys who would keep the lights on. And would help in tech evaluation of products.

The CIOs, on the other hand, are busy discussing how they would effectively drive transformation. The lead story, CIO-CEO relationship is based on the CIOs' viewpoint with this implicit assumption that they would drive it.

The hypothesis is: If technology is becoming more pervasive, the role of the person in charge of technology would only become more important.

In reality, the real question could be: Is technology becoming too important to leave it to the technologists?

There are at least half a dozen other CXOs positions that are vying for responsibilities directly concerning technology.

The most important among them is Chief Digital Officer—a position created to drive transformation and as mentioned above, they are being occupied by core business guys.

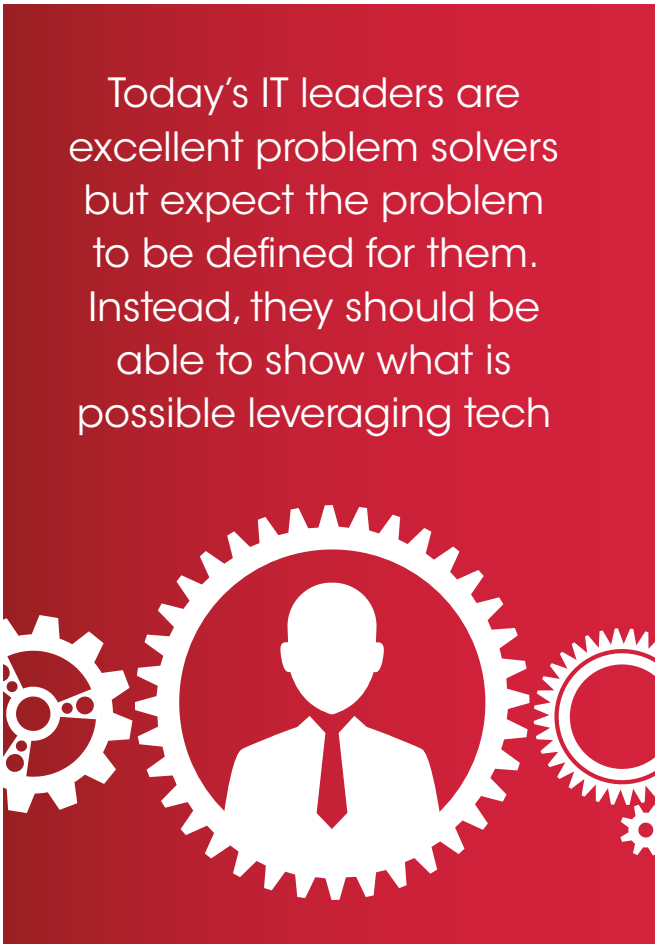
The next most prominent position is that of Chief Data Officer (also abbreviates to CDO) who are to deal with analysis of data for business insights and decision making. Of course, this role requires a different hard skillset and typically people with statistics/mathematics background are being hired for this. But that is not justification enough for keeping this outside CIO's responsibility. The CIO does not have to have all the hard skills.

Then, there is the Chief Transformation Officer—a post created as a project role. These senior executives typically perform the same role as a Chief Digital Officer but with some difference. For one, it has a larger scope, looking at organizational transformation including aspects that do not have a direct relationship with digital. Two, often these are fixed period roles like project assignments. But many decisions concerning application of technology to business are taken by them.

Some companies too have Chief Innovation Officers, who by definition, only drive newer ideas. Since many of the new ideas are closely interwoven with technology, they take major technology decisions.

In some businesses, the Chief Strategy Officers directly look after technology. This is a trend seen in many family-owned companies where new generation family scions often start with this role.

While all these new roles are taking on part of what would otherwise have been a CIO's role, in many organizations, some of the older CXOs are grabbing some tech-based roles. The good old Chief Information Security Officer (CISO), who in most organizations are/were part of the CIO's team, are now demanding independence, arguing the IT implementation and security compliance roles often have conflict of interest. The fact that they are now expected to do a lot of compliance work is making their position stronger. The regulatory stance in industries like banking and insurance that CISOs should be independent of CIOs has encouraged CISOs in other industries to stake their claim too—to an independent role outside the CIO's control.



Here's a list of questions the new leaders should ask themselves:

a. What are the top three strategic priorities for the company?
b. How could that potentially leverage technology?
c. What are my current responsibilities?
d. Do I have enough scope for achieving (b) with all my current responsibilities?
e. If not, which out of those can be delegated? And which areas can be outsourced?
f. Which are the newer opportunities I can drive? What resources do I need?
g. Based on answers to (e) and (f), how does my role change?

Wrong priorities

It is not that CIOs are not sensitized to this changing landscape. While many hope that this is a temporary phenomenon—and play ostrich—most others agree that the CIOs must change their thinking; they must think business. They consider upskilling and speaking the language of business to be the solution to this challenge.

My considered opinion—and this is a point of view, nothing more, nothing less—is that probably the big factor is neither skill nor their ability to appreciate business issues. Many CIOs today have a very good grasp of their businesses and challenges.

I would argue that it is the attitude. Many IT leaders are still not proactive. They are role-taking managers. They are excellent problem solvers but expect the problem to be defined for them—even though in business terms. They can translate that to technology and solve the problem using tech.

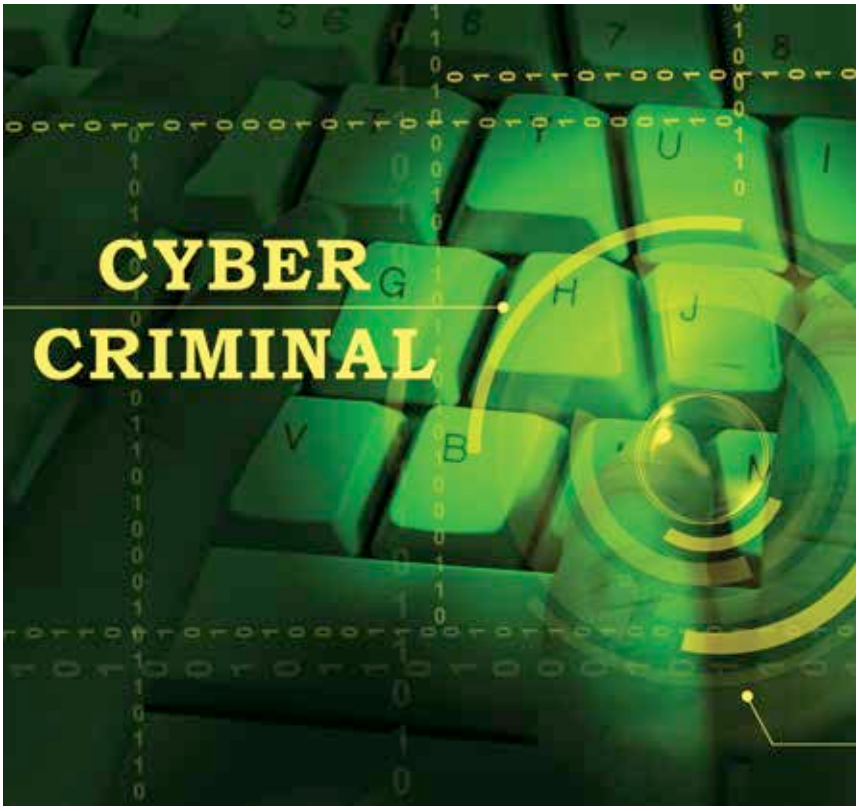
Alas, that is not enough. They should show the top managers what is possible—leveraging technology. And one thing that they should do right away—stop being apologetic about technology. Technology is the raison d'etre of their position. If anything, they should be on top of emerging technologies■

An Automated Response To Endless Zero-Days

There's an even larger treasure trove of potential vulnerabilities hidden from view that defenders haven't even begun to take into consideration as part of their security strategy

By Rajesh Maurya

The number of vulnerabilities available to cybercriminals continues to accelerate. But according to one recent report, of the over 100,000 vulnerabilities published to the CVE list, less than 6% were actually exploited in the wild. The challenge is that predicting which vulnerability will be targeted next, and which exploit will be used, requires advanced strategies, such as leveraging telemetry data to perform predictive analysis, that many organizations do not have in place.



As threats become more sophisticated, the challenges facing security personnel become more formidable. Take for example, the findings of the FortiGuard Labs 'Threat Landscape Report' from the third quarter of 2018. The FortiGuard Labs team detected close to 34,000 new malware variants – a 43% increase from the second quarter and a 129% increase over the first quarter in 2018. Zero-day attacks are becoming a more regular occurrence, and 75% of the unknown malware detected by FortiGuard Labs was not found on the VirusTotal tool – which aggregates information from 50 different antivirus vendors. As the number of exploits and vulnerabilities continues to grow, processing that burgeoning library against live traffic is becoming a burden for many of today's security solutions.

Of more concern is the fact that accelerating growth of known vulnerabilities and exploits is just the beginning of the problem. There's an even larger treasure trove of potential vulnerabilities hidden from view that defenders haven't even begun to take into consideration as part of their security strategy. Countless vulnerabilities exist inside software and hardware, particularly in the area of IoT, waiting to be discovered and exploited by cybercriminals.

Fortunately, cybercriminals have not yet figured out how to extract those zero-day vulnerabilities from existing software except in the most rudimentary ways. But that is about to change. As malicious actors begin to incorporate AI and machine learning (ML) into their exploit models, zero-day vulnerabilities and exploits will explode, and the threat landscape will be completely transformed. Attack campaigns targeting multiple zero-day vulnerabilities will be able to spin up at any instant, and cybercriminals will begin integrating more and more zero-day exploits into attack kits.

Artificial Intelligence Fuzzing (AIF) has traditionally been a sophisticated technique used in lab environments by professional threat researchers to discover vulnerabilities in hardware and software interfaces and applications. Cybercriminals will begin to leverage machine learning to develop automated fuzzing programs to accelerate the process of discovering zero-day vulnerabilities, which will lead to an increase in zero-day attacks targeting different programs and platforms.

Once AIF is in place, it can be pointed at code within a controlled environment to mine for zero-day exploits. This will significantly accelerate the rate at which zero-day exploits are developed. Once this process becomes streamlined, zero-day mining-as-a-service will become enabled, creating customized attacks for individual targets.

Historically, the price of zero-day exploits has been quite high, primarily because of the time, effort, and skill required to uncover them. But as AI technology is applied over time, such exploits will shift from being extremely rare to becoming a commodity.

We have already witnessed the commoditization of more traditional exploits, such as ransomware and botnets, and the results have pushed many traditional security solutions to their limits. The acceleration in the number and variety of available vulnerabilities and exploits, including the ability to quickly produce zero-day exploits and provide them as a service, will also impact the types and costs of services available on the dark web.

An Automated Response

The implications of such powerful and sophisticated attacks may feel overwhelming, but organizations are not helpless. Automation is available to both sides, and organizations can use automation and AI to anticipate and mitigate these advanced threats. As the number of evasive techniques multiply and the time windows for prevention, detection, and remediation continue to shrink, an automated response is essential. Organizations require a security

As malicious actors begin to incorporate AI and machine learning (ML) into their exploit models, zero-day vulnerabilities and exploits will explode, and the threat landscape will be completely transformed

platform where traditionally discrete security element can communicate with each other in real time. AI-powered communications and collaboration will enable the discovery of even the most advanced threats, dynamically deliver a proactive response to suspicious behaviour, and even begin to anticipate attacks.

However, today's security environment, too often comprise isolated security devices and poor security hygiene, will not be able to keep up. They will instead expose organizations to greater risk as they do not provide adequate visibility or controls. Instead, today's organizations require an integrated security solution that not only spans the entire distributed network environment, but also provides deep integration between each security element to automatically collect, correlate, and respond to threats in a coordinated fashion.

This is a vital first step toward addressing today's evolving threat environment and lays the fundamental foundation to protect against the threats of tomorrow. It enables actionable threat intelligence to be shared at speed and scale, shrinks the necessary windows of detection, is able to trace and intervene against attack workflows that move between network ecosystems, and provides the automated remediation required for today's multi-vector exploits.

The traditional process of identifying a threat and then developing a counter defense, or even attempting to anticipate and neutralize new attack strategies, are becoming obsolete. Defenders need to approach this problem from an entirely new direction. One possible approach is to make changes to people, processes, and technologies that impact the economic model of the attacker.

1. Deploy Deception

One economic model used by cyberattackers depends on reducing risk of discovery. Since the time between breach and exploit continues to shorten, one strategy with real potential is to simply slow down attacks. Deception strategies can generate dozens of enticing false targets combined with tripwires that force attackers to slow down, allowing attackers and malware to be quickly identified and removed.

2. Refine Threat Intelligence

Building new attacks is expensive. Instead, cybercriminals maximize their investment in an attack by making minor changes to their malware. Even something as basic as changing an IP address can enable malware to evade detection by many traditional security tools. The continued success of known exploits is testament to the effectiveness of this strategy.

As threat intelligence becomes better at identifying entire attack families, the more difficult it becomes for cybercriminals to simply adjust their existing attack tools and strategies to evade detection.

3. Take a Proactive Approach

The final approach is to engineer as much risk as possible out of your current network by moving from implicit trust to a zero trust model. This includes implementing multi-factor authentication, deploying network access control, and adopting automated, intent-based segmentation and micro segmentation. This begins by integrating traditionally isolated security devices into a single, integrated architecture. Tools that can actively correlate threat intelligence and respond as a single, integrated system are much more effective at combating even the most advanced threats.

Conclusion

Getting out of the trap of security brinksmanship requires organizations to rethink their security strategies. Instead, organizations need to target the economic motivations of cybercriminals by anticipating their attacks and thereby forcing them back to the drawing board. This starts with a cohesive security fabric that can gather and share threat intelligence, perform logistical and behavioral analysis, and tie information back into a system to pre-empt criminal intent. ■

The author is Regional Vice President, India & SAARC, Fortinet

Accelerating Business Through Customer Centricity

End customers are more attracted towards the customer-centric companies, where they get personalized services, offerings, and where their relationship is recognized and rewarded

By Susheel Sharma

Customer centricity is a reflection of our culture, process, customer experience, customer friendliness and customer satisfaction surveys. It is also an association of our product and quality services offered to our long-standing customers. According to a recent research, 89% of businesses are soon to be expected to compete mainly on customer experience. This approach will surely lead to the end goal which every company tries to achieve – 'to maximize shareholder's value'.

There's a big difference between customer centricity and good customer service. For example, customer service is to help a distressed client with your product or service, but customer centricity is more than providing good service, loyalty rewards, and special promotional offers. It is to identify the most valued customer, get a clear understanding of their requirements and delight them based on their behavior. Also, our services should fit-in as a solution to the customer's existing eco-system. We need to bring their views to the service COE (Center of Excellence), create value for them, generate revenue from them, and find more customers like them.

Customer service is to help a distressed client with your product or service, but customer centricity is more than providing good service, loyalty rewards, and special promotional offers. It is to identify the most valued customer...

Nowadays, the business process is changing dramatically, and one will find a vast difference between the modern and traditional way of doing business. End customers are more attracted towards the customer-centric companies, where they get personalized services, offerings, and where their relationship is recognized and rewarded.

Customers are willing to build long-term relationships with their providers, but the experience that they gain, decides the long-term relationship. For example, the limited taxi access and fare control has sidelined the traditional taxi business and not the taxi services like Uber. There are a few common problems with traditional business models, which include limited hours of customer service, non-personalized offerings, cost and human dependencies, and untraceable services.

Today's customers are very different in their outlook, they are more resilient, adaptable and tech savvy than their older counterparts. They are dealing with smartphones, IoT devices, and social media. They are very upfront and do not hesitate to give their feedback and reviews on social media platforms. This high volumetric customer data that comes from enterprise applications, CRM and other social media platforms, can play a crucial role in understanding and unfolding the behavioral insight, sentiment analysis and paying attention to the voice of the customer.

Organizations that take customer experience seriously will stand out and win loyal customers. Nowadays, most of the quality management system (QMS) redefine quality by emphasizing on customers' expectations and satisfaction. They are currently switching from product or service-centered approach to a customer-centric approach. Because, completely satisfied customers will speak good things and be a ready reference for the other customers. It also helps in business continuance, reducing churn and increasing revenue.

Big data and statistical techniques can facilitate enterprises that offers comprehensive powerful and actionable insights into 360° customer view, customer classification, and sentiment analysis. Analytical and statistical modeling allows an organization to forecast all portfolios and probable losses. Below are some of the key drivers:

- Identify relevant cross and up-sell opportunities
- Targeted marketing campaigns to acquire new profitable customers
- Enable the organization to understand risk dimensions faster without expanding the pool of human resources

With limited understanding of technology stack and a lack of data-centric culture being the barriers, companies should rethink and adopt the customer centric service and understand the power of data. They need to incorporate cutting-edge technologies to get interesting data and figure out ways to use customer data in the customer acquisition journey■

The author is Senior Project Manager - Business Intelligence & Analytics, 3i Infotech

CIOs Can Harness Dark Data To Boost Innovation

Dark data can help CIOs bring new revenue streams, better customer experiences, and lower business costs, says, Sanjay Agrawal, Technology Head, Hitachi Vantara

By Sanjay Agrawal

Perhaps one of the most misunderstood terms in enterprise technology is 'dark data' and it's something no CIO would want to keep in its server system. The term dark data originally coined by Gartner can be defined as "information assets which organizations collect, process, and store during regular business activities, but generally fail to use for other purposes." But despite its ominous name, it is actually a highly-valuable asset, and storing dark data and correctly mining it can provide huge benefits to businesses and help CIOs foster innovation.

The 'fairer' side to dark data

Dark data can include anything from old files to content on devices and clouds that are outside IT's immediate control and management. Dark data can appear in both structured and unstructured data, with majority of data in the unstructured segment being dark and less than 0.5% being analyzed. Majority of business data is structured data whereas unstructured data includes human and machine

data. Unstructured data is not only significantly larger than structured data but also growing many times faster. This type of data is mostly retained by enterprises by deploying huge storage, backup and management infrastructure, added to a large IT budget being spent without any business outcome.

While this data explosion is putting pressure on IT to pump in more resources to store, protect and manage the data, companies across industries are yet to understand how this data can be leveraged to achieve key business insights and avoid business risks. The bottom line being – IT is struggling to know what data they have and how their data can be leveraged for business decision making.

Enterprises dealing with their customer's personal data have another challenge of ensuring data compliance. For example, GDPR (General Data Protection Regulation) expects enterprises to ensure compliance like data protection, retention, right to forget, etc. With some part of the customer's data likely to be present in dark data, job of CIOs becomes even more challenging to ensure compliance when they have limited insights into dark data as well as limited control to apply data policies like data retention.

However, this data can be an important asset if one knows how to use it. This data could be the key to new revenue streams, better customer experiences, and lower business costs, waiting to be discovered.

What is interesting about these dark data sets is that the problems that surround them are almost always human (organizational culture or process), rather than being a specific technology challenge. Some of the key challenges enterprises face today with dark data include the ability to find effective ways to extract value from data clutters, illuminating opportunities hidden within these hidden treasure troves, implementing effective data management mechanisms and establishing active risk mitigation practices.

In a business climate where data is competitive currency, these challenges can be potential threats and pose risks to any organization's continued business health and well-being.

Business impact of dark data

Traditionally enterprises analyzed transactional business data to make business decisions but today differentiated customer experience and new business models are possible by looking at unstructured human and machine data that are related to interactions, sentiments, online behaviour, preferences, locations frequently visited, etc. For example, just sentiment analysis has given direction to enterprises for improved product and marketing strategy.

Much higher business benefits are available when enterprises start blending their human and machine data with business data dynamically that gives 360-degree view of customers. This helps knowing customers even better, create better offers and eventually more business with higher customer satisfaction. In healthcare industry, an initiative called Patient360, enables doctors get a complete unified view of all the test images, medical reports, patient profile, prescriptions, etc., that helps doctors do accurate as well as quick diagnosis, resulting in significant patient satisfaction. With such initiatives, hospitals are launching various patient services to increase the business further.

Few enterprises observed that analysis of their huge unstructured data in Hadoop systems has not resulted in desired business value. We have seen true business value become visible when CIOs start integrating their unstructured data with structured one.

The diverse mix of content from disparate sources, such as audio, video, PDFs, social feeds, IVRs and emails needs to be curated in a secure repository to improve data quality that is essential for proper analysis that can be accessed across multiple users, applications and workloads on premise or cloud. Lack of data quality of unstructured data has been one of the reasons limiting analysis of such data for many enterprises.

A recent IDC survey revealed that 77% of surveyed Indian enterprises are storing data with the hope that in the next two years they will be able to use analytics to gain business insights from this data. However, according to an analysis by Harvard Business Review, less than half of an organization's structured data is used in making business decisions, and less than 1% of unstructured data is used in any way at all. In the earlier days, banks used to create their customer's profile by looking at all the business transactions across their product lines and delivery channels. Today, banks are embarking on a journey wherein customer profiles are not only created from the business that their customers do with banks, but also from their daily interactions, sentiments, preferences, online behavior, etc.

This new process of analyzing and storing relevant data leads to achieving competitive differentiation, increased customer loyalty, deriving valuable business insights by bringing structure to data and eventually helps banks take more informed decisions in areas, such as customer retention, offers, etc., that was previously hidden in the pools of dark data that resided in the system. Thus, combating the challenges put forth by dark data and help illuminate the data at the end of the tunnel■

The author is Technology Head, Hitachi Vantara

Rethink Security With Zero Trust

At a time when companies are looking to hire more remote workers, CIO/CISOs believe it's time to rethink security with Zero Trust and multifactor authentication, finds a new study

By Sohini Bagchi

As organizations are working with newer technologies and geographically distributed teams today, they are looking to hire more contractors and remote workers without any strict requirements for physical presence in offices. While this trend of recruiting fosters collaboration and workplace productivity, it often engages in a tug-of-war with security, as the key challenge with remote workers lies in securing access to sensitive systems and data for which CIO/CISOs are often left at a crossroads. A recent report released by Okta, shows how approaches such as Zero Trust and Multifactor authentication are helping technology/security leaders rethink security in their organizations.

Why security is the No. 1 priority

In its recent survey of 1,050 decision makers including CIO/CTO/CISO and others leading the technology functions in organizations, Okta finds that 63% respondents said they are eyeing an increase in the number of remote workers (including contractors) as companies are utilizing the time saved

by avoiding long commutes to increase employee productivity, as well as work-life balance. In contrast, such a strategy entails an element of risk. Some 45% of respondents pointed to security as the biggest factor preventing them from hiring more contractors, while 39% said they see remote workers as a security threat.

The cost of a data breach — both financially and in terms of brand reputation — is growing. A separate study done by Ponemon Institute, titled *2018 Cost of a Data Breach Study* found that on average, companies took 197 days to identify a data breach and 69 days to contain it. The time required to identify and contain breaches were highest for malicious and criminal attacks and lower for breaches caused by human error. Needless to say then that security should be part of an organization's mission statement.

As Dr O. A. Balasubramaniam, Sr. Vice President–IT at Roots Group of Companies, states, "Technology advancement has changed the workplace scenario, and information is one of the most valuable assets to every organization, yet often one of the most vulnerable one."

He believes that as there is a direct economic cost of such attacks to the business, such as theft of corporate information, disruption to trading, and repairing costs of systems as well as reputational damage to organizations, all businesses, no matter its size, needs to ensure the proper knowledge on cyber security, tools involved, up-to-date on the latest cyber security threats and the best methods for protecting data.

"Cyber attacks could irreparably damage the business, so security needs to be the top priority," Balasubramaniam adds.

Therefore, with these new ways of working, companies need to move beyond traditional security parameters.

Enter Zero Trust, MFAs

To respond to security threats, Okta study found more companies are looking at Zero Trust, a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.

John Kindervag, Field CTO at Palo Alto Networks, who created the concept of Zero Trust, coined the term, and promoted the approach while serving as a vice president and principal analyst at Forrester Research, approaches Zero Trust from a unique position. He mentions in a recent security roundtable, "Although the idea is fairly straightforward— trust is the root cause of all data breaches and most other negative cyber-security events; we don't need trust in digital systems when the only beneficiaries are attackers—putting the concept into motion can prove challenging."

In today's security landscape, it's no longer about the network — it's centered on the people who access your systems, and the identity access controls for those individuals

Going by this concept of security approach, Okta researchers found that one-third of respondents said they already have a formal strategy for Zero Trust and are actively working to secure their companies with this approach. Another 25% said they're creating a formal plan out of a Zero Trust strategy, while 24% said they're considering it but don't yet have any formal plans to implement it.

In today's security landscape, it's no longer about the network — it's centered on the people who access your systems, and the identity access controls for those individuals. And therefore, the road to Zero Trust is paved with strong multi-factor authentication (MFA), states the study researchers.

Some 61% of respondents said they use security questions, while 54% have implemented software-based one-time passwords. A little over half the CIO/CTO/CISOs use SMS, voice verification, and/or the emailing of one-time passwords, with 36% adopting physical keys and U2F (Universal 2nd Factor) tokens.

Among the different MFA methods, one-time passwords provided by software, physical and U2F tokens and biometrics are considered the strongest, while security questions and one-time passwords provided on email are seen as the weaker lot.

The stark reality

The survey also found a strong disconnect between how quickly respondents expect to respond to a security breach and the reality of how long such responses can actually take. Some 73% of respondents said they expected their company would identify a security compromise immediately or within 24 hours, while 78% said they would respond to such a breach immediately or within 24 hours. Further, 60% of respondents said they're very prepared to handle a security breach.

The worrisome finding is that CIOs are particularly confident in their company's preparedness and so are the respondents from some of the most vulnerable industries, including technology, financial services, manufacturing, retail, and healthcare.

As the Okta report states, "The gulf between expectations and reality shows why security can be such a challenge even for the world's largest companies."

Nonetheless, pursuing Zero Trust strategy and using any of the strong MFA types can surely reduce the burden of technology leaders in securing the remote workers and likewise the enterprise to a large extent.■

AI – Transforming Customer and Employee Experience

Studies show, AI is viewed by organizational leaders as a strategic advantage to customer and employee experience

By Sohini Bagchi

In recent times, the biggest challenge for Indian businesses is keeping up with changing consumer expectations. While companies are striving to offer more information, greater personalization and a brand new experience to the digitally-savvy consumers, they often fail to meet the expectations of their customers. A new study by Salesforce researchers shows that strategic use of technologies, such as Artificial Intelligence (AI), chatbots and mobile can guarantee a more enhanced customer experience.

In India, 93% of CIOs and other decision makers believe their company's customer service must transform in order to stay competitive, according to the study, titled '2019 State of Service Report' capturing insights and trends from decision makers worldwide to determine their biggest challenges and priorities. The tech decision makers also state that improving service technologies is a top priority, followed by upgrading workforce skills and lastly revamping processes and workflows.

In this context, AI is viewed by CIOs as a strategic advantage to customer and employee experience.

Even though AI adoption is nascent in the country, the study sees the technology is set to soar as more teams turn to chatbots, text and voice analytics, and other use cases. In India, the use of AI and Chatbots by customer service teams is projected to increase by 90% and 118% respectively, over the next 18 months, said the study.

For example, insurance companies, once considered laggards in the use of technologies, are using AI and chatbots to deliver faster, better and seamless customer experience. As Mehmood Mansoori, Member of Executive Management & Group Head - IT & Online Business at HDFC General Insurance explains. "The extensive use of AI-based Chatbots has helped us in improving auto adjudication of claims tremendously, speeding up claim settlement at the moment of truth. It has also enhanced customer experience by creating an omni-channel to onboard customers – improving engagement across platforms leading to much greater productivity and efficiency."

Not only in insurance, AI is powering nearly every experience we have—making it smarter, seamless and personalized. AI-powered technologies are making its way to every business, across all industries, delivering real personalized value, in real-time. It is little wonder that industries, such as healthcare, banking and financials, ecommerce, IT and customer care, among others too are heavily relying on AI-based chatbots and virtual assistants to improve their bottomline and boost customer experience.

Trained service agents to lead the growth

As CIO and technology leaders are making service a strategic asset, the study shows that companies are increasingly investing on service agents. The results are also paying off well.

"The service agent of today is increasingly tasked with building relationships and driving revenue. They are swapping their mundane tasks for challenging, high-value work," Salesforce researchers say. 89% of agents in India said their roles are more strategic than two years ago and executives increasingly understand that customer service transformation requires an investment of time, talent, and resources; 85% of Indian decision makers are making significant investments in agent training and 94% of service agents in India say they have a clear path for career growth at their job.

The Salesforce report further notes that service is moving beyond the call center as customers embrace an array of digital channels. 88% of service professionals in India say their organization is seeing increased case volume through digital channels.

Indeed, the steady progress toward deeper implementation of AI in the contact center is inevitable because it will allow organizations to improve service levels and reduce costs. Another recently concluded survey by Xerox states that 42% technology decision makers predicted in the survey that the contact center as they know it now will cease to exist by 2025. In such a scenario, those implementing AI and bots into their contact center would be the ones to stay afloat.

Mobile workforce - a differentiator

The expanding mobile workforce is driving new revenue streams and brand differentiation. Arming mobile workers with the same capabilities as their office-based colleagues is viewed as key to this evolution. 96% of Indian CIOs and tech decision makers believe the experience a customer has with a mobile worker is a reflection of their brand. Over 69% have increased mobile worker headcount over the past year and 78% expect to increase mobile worker headcount next year.

"Businesses are realizing that service can drive elevated customer experiences, differentiate brands, and drive new revenue streams. As a result, service leaders are investing in their people, processes, and technology to drive nothing short of a transformation," Sunil Jose, Senior Vice President and Country Leader, Salesforce India observes.

Key takeaways for the CIO

While the Salesforce study focuses on improving customer experience with AI, helping CIOs make informed decisions, several other studies conducted in the recent past emphasize the importance of AI in the enterprise. As per a prediction made by IDC (International Data Corporation), by 2019, 40% of digital transformation initiatives will be supported by some sort of cognitive computing or AI effort. Another study by Gartner says by 2020, 85% of customer interaction will be managed without a human.

However, experts emphasize on human skills too that will make AI adoption relevant. At the MIT Sloan CIO Symposium, David Gledhill, group CIO and head of group technology and operations for DBS Bank, mentions that even though AI has an "aura of complexity" around it but, like any tool, a big part of demystifying AI will be in training people to understand what it can and can't do," he says adding that digital and technology leaders have a big role to play here.

For the digital CIO, the key takeaways from these researches include:

First, CIOs should realize customer experience is a major competitive differentiator and they should view customer service as the primary vehicle for improving the customer experience. For this a shift in their role is necessitated.

Second, CIOs and Chief digital officers (CDOs) should explore AI-led tools and applications to offer unique customer service that is personalized, always on and real-time, consistent and omni-channel.

Finally, in order to lead customer experience transformation, they must convince the CEO and board to embrace, deploy and utilize AI technologies across organizations.■

DNS Hijack – Simplifying The Misroute

DNS hijacks are rapidly becoming common and are posing big threat to e-commerce, corporates and end users. What exactly is a DNS hijack, how does it work and how to safeguard against the threat?

By Archie Jackson

You have read about DNSpionage. The hackers behind DNSpionage succeeded in compromising key components of DNS infrastructure of more than 50 Middle Eastern companies and government agencies, including targets in Albania, Cyprus, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Saudi Arabia and the United Arab Emirates.

The passive DNS data shows the attackers were able to hijack the DNS records for mail.gov.ae, which handles email for government offices of the United Arab Emirates. Here are just a few other interesting assets successfully compromised in this cyber espionage campaign:

- nsa.gov.iq: the National Security Advisory of Iraq
- webmail.mofa.gov.ae: email for the United Arab Emirates' Ministry of Foreign Affairs
- shish.gov.al: the State Intelligence Service of Albania
- mail.mfa.gov.eg: mail server for Egypt's Ministry of Foreign Affairs
- mod.gov.eg: Egyptian Ministry of Defense
- embassy.ly: Embassy of Libya
- owa.e-albania.al: the Outlook Web Access portal for the e-government portal of Albania
- mail.dgca.gov.kw: email server for Kuwait's Civil Aviation Bureau
- gid.gov.jo: Jordan's General Intelligence Directorate
- adpvpn.adpolice.gov.ae: VPN service for the Abu Dhabi Police
- mail.asp.gov.al: email for Albanian State Police
- owa.gov.cy: Microsoft Outlook Web Access for Government of Cyprus
- webmail.finance.gov.lb: email for

Lebanon Ministry of Finance
- mail.petroleum.gov.eg: Egyptian Ministry of Petroleum
- mail.cyta.com.cy: Cyta telecommunications and Internet provider, Cyprus
- mail.mea.com.lb: email access for Middle East Airlines

What exactly is a DNS?

The domain name system (DNS) functions as an interpreter between humans, who talk words, and computers that talk numbers.

DNS is the keeper of all domain names that are registered on the internet. Its job is to translate those names into IP addresses and hence show the relevant website to the user. Whenever we want to visit a website, it simply matches the name with the IP address and shows the result. This process may take place through a local cache or through a zone file that is present on the server. A zone file is a file on the server that contains entries for different Resource Records (RR). These records can provide us a bunch of information about the domain. Let's say the user opens up the browser and types in citibank.com. It is now the responsibility of the DNS resolver in the user's operating system to fetch the IP Address. It first checks it's local cache to see if it can find a record for the queried domain name. A local cache usually contains a mapping of IP-addresses to hostnames which are saved during recent lookups so that the DNS resolver does not have to fetch the IP address again and again. If it can't find the IP address in it's cache it queries the DNS server to see if it has a record for it. A DNS server is usually given to the end user by the ISP (Internet Service Provider) or you can manually set up a DNS server for yourself. If it still can't find the IP Address then it goes through a process or recursive DNS query in which it queries different nameservers to get the IP-address of the domain. As soon as it finds the IP-address it returns the IP-address back to the user and also caches it for it's future use.

Example, using nslookup

```
> set type=a
> google.com
Server:         10.0.1.1
Address:        10.0.1.1#53

Non-authoritative answer:
Name:   google.com
Address: 74.125.236.84
Name:   google.com
Address: 74.125.236.82
Name:   google.com
Address: 74.125.236.80
Name:   google.com
Address: 74.125.236.81
Name:   google.com
Address: 74.125.236.83
```

In the second line we have set the type = a. This will query the A records and return us an IP-address for the domain we query. When we type in google.com we get an output showing the server and an IP-address#port. This server is the current DNS server that is serving our request. DNS uses UDP port 53 to serve its requests. The third line in the output shows "Non-authoritative answer". We can see all the IP-addresses associated with google.com. This is usually the case with large organizations where they use multiple servers to manage scalability of request traffic.

A Zone file is basically a text file present on the server hosting the domain that contains entries for different resource records.

Different types of Resource Records exist within a Zone file:
- A Records – Maps an IP Address to a hostname. For example, 74.125.236.80 for google.com.
- NS Records – Delegates a given zone to use the given authoritative nameserver. For example, ns1.google.com is an authoritative nameserver for google.com
- MX Records – This tells us which server is responsible for receiving mails sent to that domain name.
- TXT Records – This consists of arbitrarily human readable text in a record.
- CNAME Records – Gives an alias of one name to another.

How does a DNS hijack work?

DNS Hijacking is when bad actors redirect or "hijack" DNS addresses and reroute traffic to bogus DNS servers. Once a DNS address is successfully hijacked to a bogus DNS server, it translates the legitimate IP address or DNS name into the IP addresses of the hacker's malicious website of choice.

DNS spoofing and DNS poisoning (or DNS cache poisoning) are the same thing, but slightly different than DNS hijacking. In the latter, the hacker would either plant a malware or hack the router DNS settings. However, in DNS poisoning or spoofing, the hackers compromise (poison) the cache of a DNS server.

DNS redirect, on the other hand, is an unethical way of redirecting users to unintended pages such as advertisements pages, etc. ISPs are the ones that usually practice DNS redirect to drive users, say from a 404 page to their desired pages which are usually ad pages. It wouldn't be unfair to name it ISP DNS hijacking.

If your computer has been infected by a malware that managed to change your PCs DNS settings, it will no longer have the ability to correctly make the connection between a user-friendly domain name and its original IP address. This means that you will be directed to fake versions of certain websites you are trying to visit. Your computer's DNS settings are usually assigned by your ISP (Internet Service Provider). When you try to access a website, your computer refers your request to those settings which redirects it to a DNS server. The server matches the name with the IP address and then sends you to the desired website. If your computer settings are compromised, your request will be redirected to a rogue DNS server. Consequently, the rogue server will translate your request into a fake IP address that leads to a fake or malicious website.

DNS is highly decentralized. No single DNS server holds all the IP addresses and their corresponding domains. Your query will travel along

a chain of DNS servers before you get your result. Therefore, DNS hijacking is the practice of redirecting DNS queries. You send out a query, but a third party steers the query the wrong way. As a result, you get a false IP address, and the wrong page loads on your screen. A DNS hack could happen at any link in the chain of DNS queries. Here's how:

- **Malware:** Your computer or router can be infected with malware that rewrites the configuration of DNS settings. As a result, your device queries a conned DNS server that serves you fake IP addresses. A malicious malware could redirect you through hacker-controlled open web proxies and get access to all your traffic and could also be directed to a dummy website that extracts your passwords and usernames through fake login procedures.
- **Compromised DNS server:** In this, your query is redirected in the wrong destination by a DNS server under a hacker's control. This attack is even more clever because once the query leaves your device, you have no control whatsoever over the direction your traffic takes.
- **Internet service provider interference:** Some internet service providers use DNS hijacking on their own users to display ads or collect statistics. They do this by hijacking the NXDOMAIN response. NXDOMAIN is the response you get if you type in a domain that does not exist (meaning it doesn't have a corresponding IP address). For example, if you entered "ssdsrfadsfdgfaaf.com" into your browser, you would get the NXDOMAIN response: "The website cannot be found" or a similar error message. When an internet service provider hijacks the NXDOMAIN response, they replace the error message with a fake website set up by the internet service provider to show you ads or collect your data.

Detecting DNS hijacking

The fastest way to detect DNS hijacking is by using the ping utility. If you ping a non-existent domain and it resolves, that is probably a very strong indicator that your ISP is hijacking your DNS traffic. The idea here is to ping the hostname, this should fail if it does actually return an IP address you are the victim of DNS hijacking. Another way which gives you a 100% confirmation if your DNS is being hijacked is to change your DNS address on a device you use to 0.0.0.0 and 0.0.0.1. If after that your Internet still works and you can open up web pages normally, your DNS traffic is hijacked.

How to protect

- **Be aware of the issue:** Like with most things, the first step would be to become aware of the issue and to try and find out if you've already been affected by a DNS changer. The easiest way to detect a DNS hijack is to use the ping utility. Try pinging a domain you know for sure doesn't exist and if it resolves, there is a very high chance that you are a victim of DNS hijacking.
- **Stay away from shady websites:** Considering that in many cases, the attacks are carried out through trojan horse or similar malware programs, it is highly recommended to stay away from shady websites in the first place. The viruses are usually served through video or audio codecs, through Youtube downloaders or other similar free online utilities. A great example is the DNS Changer Trojan which was used to hijack over 4 million computers.
- **Change your router password:** Changing your router password constantly also decreases your chances of being hijacked. If a hacker targeted your router and is trying to access it to change the settings, it would be best not to find that it is only protected by the default factory password.
- **Use a VPN service:** Using a VPN service is also one of the most common and effective ways of protecting yourself against DNS hijacking. A VPN would encrypt all your internet traffic and send it through a virtual tunnel. Since this includes all your DNS/Web traffic, your hijacker will be unable to decipher your traffic, which in the end means that you will not have to deal with any annoying or dangerous redirects. On top of this, you can use a VPN regardless of your location, which means that you can stay protected while you travel or while using less secured Wi-Fi networks. Some of those best practices for organizations include:
- Use DNSSEC (both signing zones and validating responses). DNSSEC protects applications from using forged or manipulated DNS data, by requiring that all DNS queries for a given domain or set of domains be digitally signed. In DNSSEC, if a name server determines that the address record for a given domain has not been modified in transit, it resolves the domain and lets the user visit the site. If, however, that record has been modified in some way or doesn't match the domain requested, the name server blocks the user from reaching the fraudulent address. While DNSSEC can be an effective tool for mitigating attacks such as those launched by DNSpionage, only about 20% of the world's major networks and Web sites have enabled it, according to measurements gathered by APNIC, the regional Internet address registry for the Asia-Pacific region.
- Use registration features like Registry Lock that can help protect domain names records from being changed
- Use access control lists for applications, Internet traffic and monitoring
- Use 2-factor authentication, and require it to be used by all relevant users and subcontractors
- In cases where passwords are used, pick unique passwords and consider password managers
- Review accounts with registrars and other providers
- Monitor certificates by monitoring■

The author is AVP – Technology/ Information Security at Genpact

Here's How Healthcare CIOs Can Brace Up Against Cyber Threats

A panel of healthcare CIOs and technology suppliers discussed the challenges and opportunities for healthcare CIOs

By Sohini Bagchi

It is no secret that ransomware and other cyberattacks are rising phenomenally across the world, attacking every industry sector possible and healthcare is one of the biggest targets. While the good news is, the healthcare sector is relying on technology that's connected to the internet: From patient records and lab results to radiology equipment –facilitating patient care and engagement and clinical support; bad news is that those technologies, such as Artificial Intelligence (AI) and Internet of things (IoT) are often vulnerable to cyberattacks, siphoning off patient data, attacking hi-tech medical systems, or shutting down an entire hospital until a ransom is paid.

And now the worst news – despite the rising threat, the vast majority of hospital CIO/CISOs and physicians are not in a position to handle cyber security threats, even though they pose severe threats to patients, doctors and the entire healthcare organization.

At a recent CIO forum on 'Cyber Security in Healthcare', organized by the Bengal

Chamber of Commerce and Industry (BCC&I) with Medica Hospitals and PwC, CIOs and IT experts in healthcare raise some pertinent issues faced by the sector. They also highlight strategies to improve cyber security in healthcare organizations.

"Despite suffering from ransomware attacks, organizations remain unprepared for the next round of large-scale attacks," said Vivek Mahadevan, Head - Healthcare Sales, NTT Data India. Quoting a Ponemon report on cyber security breaches in healthcare, he said that data breaches cost the healthcare industry USD 363 per exposed record, more than twice the average across all industries, and this needs special attention.

There are several challenges CIOs at many healthcare firms are facing at the moment, most importantly, they often fail to secure the funding for cyber security. "While attacks are becoming increasingly difficult to identify, prevent and mitigate, in mid-sized hospitals, underinvestment in cybersecurity has left many so exposed that they are unable to even detect cyberattacks when they occur," according to Gunjan Kumar, CIO and Head New Initiatives, Regency Healthcare.

"The result is that while attackers may compromise an organization within a matter of seconds or minutes, it often takes many more weeks and sometimes months – before the breach is detected, damage is contained and defensive resources are deployed to prevent the same attack from happening again," he stated.

Moreover, as organizations seek to protect their patient information from these growing threats, demand for healthcare professionals who are familiar with the current state of cyber security in healthcare is on the rise. However, Sheryl Jose, Head - Cyber Security, Emcure Pharma Group, observed a wide demand-supply gap as far as trained security personnel are concerned.

"The healthcare cyber security IT shortage is probably due to many hospitals' inability to meet the pay rates like their peers in the financial services sector, which is generally protected by considerably more robust cybersecurity than healthcare," he mentioned, adding that the big hospitals are probably okay with attracting people and paying for the software and technology, but the smaller and mid-sized ones continue to reel under the crisis.

The panelists also agreed that one of the biggest challenges is that employee awareness and attentiveness to security is still an issue. As Girish Kumar, Vice President - Operations, Welcare Health Systems, noted, lack of basic security awareness among staff as well as state-of-the-art cybersecurity solutions has made the healthcare industry a favorite target for hackers. "If that's done properly, the cyber security scenario in healthcare organizations is bound to improve."

The panelists also agree on some of the most common threats that continue to haunt healthcare, which are:

- **Malware and ransomware:** Cyber criminals use malware and ransomware to shut down individual devices, servers or even entire networks. In some cases, a ransom is then demanded to rectify the encryption.
- **Cloud threats:** An increasing amount of protected health information is being stored on the cloud. Without proper encryption, this can be a weak spot for the security of healthcare organizations.
- **Misleading websites:** Clever cyber criminals have created websites with addresses that are similar to reputable sites.
- **Phishing attacks:** This strategy sends out mass amounts of emails from seemingly reputable sources to obtain sensitive information from users.

- **Encryption blind spots:** While encryption is critical for protecting health data, it can also create blind spots where hackers can hide from the tools meant to detect breaches.
- **Employee error:** Employees can leave healthcare organizations susceptible to attack through weak passwords, unencrypted devices and other failures of compliance.

Kumar also highlighted that another growing threat in healthcare security is found in medical devices. As pacemakers and other equipment become connected to the internet, they face the same vulnerabilities as other computer systems. To ensure patient safety, he recommends that both the manufacturer that creates the device and the healthcare facility that implants it take preventive security measures.

Strategies for improving cyber security

The panelists said due to the significant financial impact of data breaches in healthcare, CIOs/CISOs and the top management in medical organizations can play an important role in ensuring that they remain secure. As Shuvankar Pramanick, CIO, Sir Ganga Ram Hospital said, technology professionals in healthcare are continually developing new strategies and best practices to ensure the safety of sensitive health data, protecting both the patient and organization from financial loss and other forms of harm. "However, much is left to be done," he added.

From the discussion, here are the takeaways for CIOs and IT leaders to help healthcare organizations improve their cyber security by implementing the following practices:

- **Establish a security culture:** Ongoing cyber security training and education emphasize that every member of the organization is responsible for protecting patient data, creating a culture of security.
- **Protect mobile devices:** An increasing number of healthcare providers are using mobile devices at work. "Encryption and other protective measures are critical to ensure that any information on these devices is secure," says Jose.
- **Train staff on handling computers:** New employee on-boarding should include training on best practices for computer use, including software and operating system maintenance.
- **Use a firewall:** Anything connected to the internet should have a firewall.
- **Install and maintain anti-virus software:** Simply installing anti-virus software is not enough, says Pramanick. According to him, continuous updates are essential for ensuring healthcare systems receive the best possible protection at any given time.
- **Have a Plan-B:** Files should be backed up regularly for quick and easy data restoration. Organizations should consider storing this backed-up information away from the main system if possible and have a plan B in case of any failure.
- **Control access to confidential health information:** Access to protected information should be granted to only those who need to view or use the data.
- **Use strong passwords and change them regularly:** The Verizon report found that 63% of confirmed data breaches involved taking advantage of passwords that were the default, weak or stolen. Mahadevan notes, healthcare employees should not only use strong passwords, but ensure they are changed regularly.
- **Limit network access:** Any software, applications and other additions to existing systems should not be installed by staff without prior consent from the proper organizational authorities.
- **Control physical access**: Data can also be breached when physical devices are stolen. Computers and other electronics that contain protected information should be kept in locked rooms in secure areas.

As organizations seek to protect their patient information from growing threats, demand for healthcare professionals who are familiar with the current state of cyber security in healthcare is on the rise

Like with any other industry, cyber security in healthcare isn't going to improve overnight. As experts believe, it's going to take ongoing commitment, by many organizations working together, for patient protection to improve. Therefore fundamental practices, like staff members informed about potential scams and the importance of changing passwords regularly, can go a long way towards healthcare organizations better securing their networks and the onus lies on CIO/CISOs who are the custodian of this change■

Majority Of Organizations Still Vulnerable to Cyberattacks

77% of respondents indicated they do not have a cybersecurity incident response plan applied consistently across the enterprise

A vast majority of organizations surveyed are still unprepared to properly respond to cybersecurity incidents, with 77% of respondents indicating they do not have a cybersecurity incident response plan applied consistently across the enterprise, according to a study conducted by the Poneman Institute, on behalf of IBM.

While studies show that companies who can respond quickly and efficiently to contain a cyberattack within 30 days save over USD 1 million on the total cost of a data breach on average, shortfalls in proper cybersecurity incident response planning have remained consistent over the past four years of the study. Of the organizations surveyed that do have a plan in place, more than half (54%) do not test their plans regularly, which can leave them less prepared to effectively manage the complex processes and coordination that must take place in the wake of an attack.

The difficulty cybersecurity teams are facing in implementing a cyber security incident response plan has also impacted businesses' compliance with the General Data Protection Regulation (GDPR). Nearly half of respondents (46%) say their organization has yet to realize full compliance with GDPR, even as the one-year anniversary of the legislation quickly approaches.

"Failing to plan is a plan to fail when it comes to responding to a cybersecurity incident. These plans need to be stress tested regularly and need full support from the board to invest in the necessary people, processes and technologies to sustain such a program," said Ted Julian, Vice President of Product Management and Co-Founder, IBM Resilient. "When proper planning is paired with investments in automation, we see companies able to save millions of dollars during a breach."

Other takeaways from the study include:

- **Automation in Response Still Emerging – l**ess than one-quarter of the respondents said their organization significantly uses automation technologies, such as identity management and authentication, incident response platforms and security information and event management (SIEM) tools, in their response process.
- **Skills Still not Paying the Bills –** only 30% of respondents reported that staffing for cybersecurity is sufficient to achieve a high level of cyber resilience.
- **Privacy and Cybersecurity Tied at Hip –** 62% of respondents indicated that aligning privacy and cybersecurity roles is essential or very important to achieving cyber resilience within their organizations.

Automation still emerging

For the first time, this year's study measured the impact of automation on cyber resilience. In the context of this research, automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. These technologies depend upon artificial intelligence, machine learning, analytics and orchestration.

When asked if their organization leveraged automation, only 23% of respondents said they were significant users, whereas 77% reported their organizations only use automation moderately, insignificantly or not at all. Organizations with the extensive use of automation rate their ability to prevent (69% vs. 53%), detect (76% vs. 53%), respond (68% vs. 53%) and contain (74% vs. 49%) a cyberattack as higher than the overall sample of respondents.

According to the *2018 Cost of a Data Breach Study*, the use of automation is a missed opportunity to strengthen cyber resilience, as organizations that fully deployed security automation saved USD 1.5 million on the total cost of a data breach, contrasted with organizations that did not leverage automation and realized a much higher total cost of a data breach.

Skills gap still impacting cyber resilience

The cybersecurity skills gap appears to be further undermining cyber resilience, as organizations reported that a lack of staffing hindered their ability to properly manage resources and needs. Survey participants stated they lack the headcount to properly maintain and test their incident response plans and are facing 10-20 open seats on cybersecurity teams. In fact, only 30% of respondents reported that staffing for cybersecurity is sufficient to achieve a high level of cyber resilience. Furthermore, 75% of respondents rate their difficulty in hiring and retaining skilled cybersecurity personnel as moderately high to high.

Adding to the skills challenge, nearly half of respondents (48%) said their organization deploys too many separate security tools, ultimately increasing operational complexity and reducing visibility into overall security posture.

Privacy growing as a priority

Organizations are finally acknowledging that collaboration between privacy and cybersecurity teams can improve cyber resilience, with 62% indicating that aligning these teams is essential to achieving resilience. Most respondents believe the privacy role is becoming increasingly important, especially with the emergence of new regulations like GDPR and the California Consumer Privacy Act, and are prioritizing data protection when making IT buying decisions.

When asked what the top factor was in justifying cybersecurity spend, 56% of respondents said information loss or theft. This rings especially true as consumers are demanding businesses do more to actively protect their data. According to a recent survey by IBM, 78% of respondents say a company's ability to keep their data private is extremely important, and only 20% completely trust organizations they interact with to maintain the privacy of their data.

In addition, most respondents also reported having a privacy leader employed, with 73% stating they have a Chief Privacy Officer, further proving that data privacy has become a top priority in organizations■

Organizations Failing To Protect Cloud Data Effectively

Data protection is becoming more challenging to achieve with the rise of multi-cloud and multi-site backup

A recent research by Barracuda's study, titled 'Closing Backup and Recovery Gaps' reveals new details about the attitudes and approaches SMBs have when it comes to backing up and recovering data, the impact that cloud and SaaS solutions are having on data protection strategies, and confusion that is exposing firms to significant risk. Barracuda surveyed more than 1,000 IT professionals, business executives, and backup administrators worldwide to find out more about their data protection strategies.

Backup challenges and confusion

Overall the study shows that the migration to the cloud is well underway, but organizations are not protecting their cloud and SaaS data effectively. Key findings include:

- Data protection is becoming more challenging to achieve with the rise of multi-cloud and multi-site backup.
  - 57% of respondents are responsible for backing up more than two sites
  - 35% are using multiple cloud services
- IT decision makers are warming up to the cloud, and the use of the cloud as a secondary backup location is on the rise.
  - 64% of global organizations say they replicate backup data to the cloud
  - 36% still do not follow this best practice
- IT teams view email, SQL, and proprietary application data as the most common workloads to protect with backup, but SaaS data is not viewed as critical, which puts business continuity at risk.
  - Only 16% of respondents report that they back up their SaaS data.
- Office 365 is one of the most popular cloud-based productivity platforms, but Office 365 confusion is exposing firms to significant risk
  - More than 60% of SMBs are using Office 365 to drive business success
  - 40% are not using any third-party backup tools to protect mission-critical data because they believe Office 365 provides all the backup they need, which is unlikely to be true

"While more IT professionals are embracing ways the cloud can support data protection, such as replicating backup data to the cloud, many are making dangerous assumptions about SaaS and cloud data that are putting organizations at risk," says Chris King, Director, Product Management, Data Protection at Barracuda Networks. "IT still needs to consider how data is protected, even after migrating to cloud or SaaS applications."

Today's complex infrastructures and targeted cyber attacks require a complete backup strategy that protects data wherever it resides — on-premises or in the cloud. Barracuda's Backup solutions offer continuous data protection and the flexibility of replicating to a remote physical or virtual appliance, or to the cloud. Its Cloud-to-Cloud Backup provides comprehensive, cost-effective and scalable protection■

Mobile Apps Will Largely Impact Businesses By 2020: Gartner

Conversational applications are the second-most widely developed type of application at 73% for voice apps and 60% for chatbots

As user application touchpoints increase in frequency, change in modalities and expand in device type, the future of app development is multi-experience, according to a recent survey by Gartner.

"Development platform vendors are expanding their value proposition beyond mobile apps and web

development to meet user and industry demands," said Jason Wong, research vice president at Gartner. "The result is the emergence of multi-experience development platforms, which are used in developing chat, voice, augmented reality (AR) and wearable experiences in support of the digital business."

Most common enterprise applications

Despite the web browser continuing to serve as the most popular application touchpoint, mobile apps are on the rise. As immersive devices, such as smartwatches, smartphones and voice-driven devices permeate the industry, the modes of interaction (type, touch, gestures, natural language) expand across the digital user journey.

Among enterprises that have developed and deployed at least three different types of applications (other than web apps), the most common are mobile apps (91%). "These figures are higher than any other application types we asked about, and suggest that the maturity of mobile app development is necessary for expansion into other interaction modalities," said Wong.

Contrary to the perception that mobile apps are in decline, they are in the lead for applications projected to have the most impact on business success by 2020, according to respondents

Conversational applications are the second-most widely developed type of application type at 73% for voice apps and 60% for chatbots, according to the survey. "This reflects the natural evolution of application functions to support the digital user journey across natural language-driven modes and devices," said Wong.

Technology behind multi-experience development

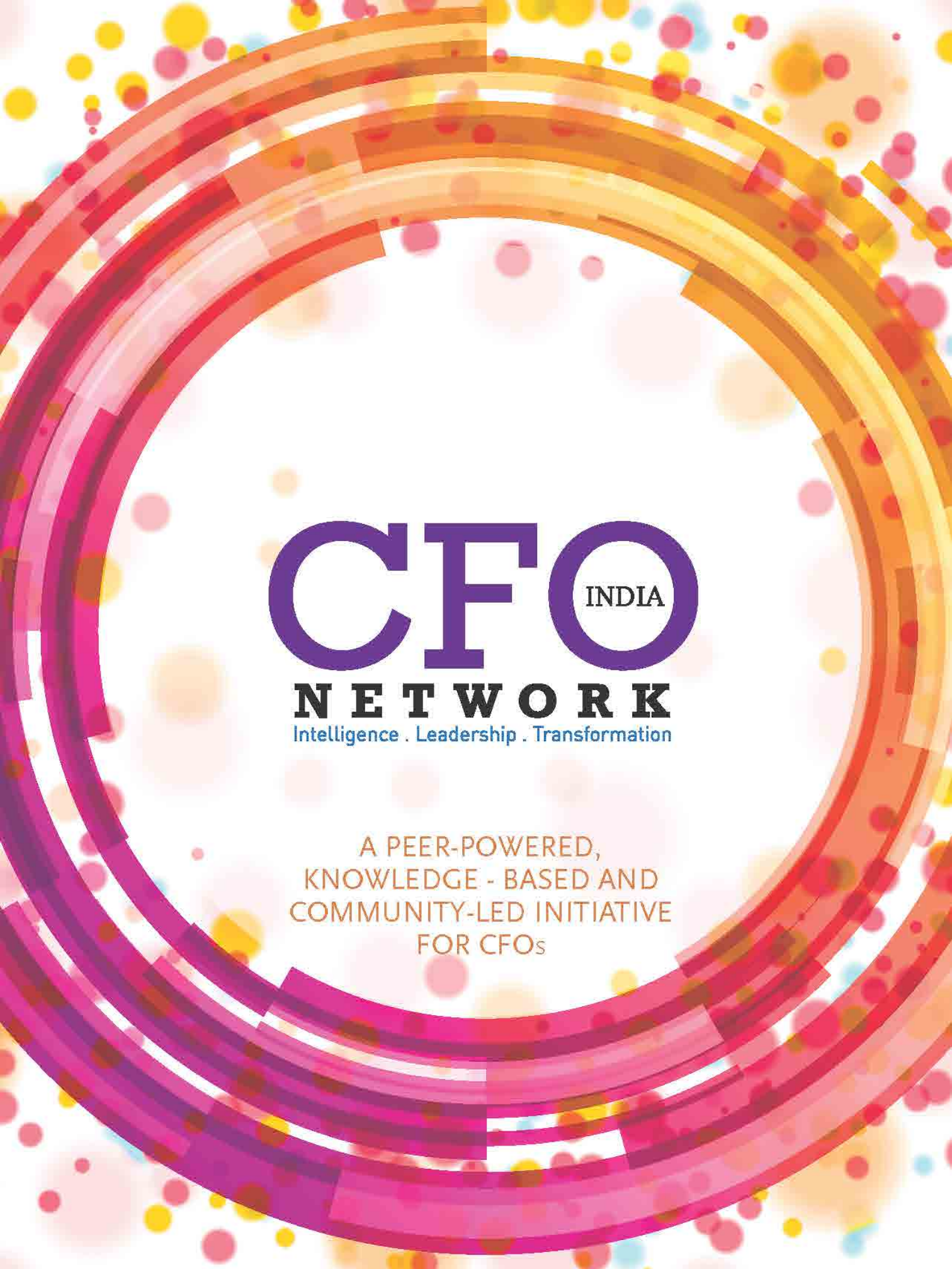
Cloud-hosted artificial intelligence (AI) services are the most widely used technology to support multi-experience application development (61% of respondents), followed by native iOS and Android development (48%) and mobile back-end services (45%). "This is consistent with the rise of conversational user interfaces, image and voice recognition and other AI services that are becoming commonplace within apps," said Wong.

Business impact behind multi-experience development

Contrary to the perception that mobile apps are in decline, they are in the lead for applications projected to have the most impact on business success by 2020, according to respondents. Following mobile apps are virtual reality (VR) applications and AR applications. "Although respondents indicated a high level of development activity for chatbots and voice apps, very few thought they'd have the most business impact by 2020," said Wong.

Barriers in developing multi-experience development

The top barrier to building compelling multi-experience applications is the need for business and IT alignment, according to nearly 40% of survey respondents. More than one-quarter of the respondents identified shortcomings in developer skills and user experience expertise as a barrier. "Skills gap in relation to emerging technologies cannot be overstated when discussing inhibitors to scaling digital initiatives, including multi-experience development strategy," said Wong■


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

Double Scoop

Two times
the revelation

Pankaj Mishra

Senior Manager - Global Technologies, Innodata

A TECH IDOL I LOOK UPTO

Steve Jobs

A PLACE WHERE I WOULD LOVE TO GO

Cairo

A FESTIVAL WHICH I LIKE THE MOST

Holi

MY FAVORITE WEB SHOW

CNBC TV18

MY FAVORITE TECH TOOL

NESSUS

MY PEER IN THE IT COMMUNITY

Alok Malik

AVP - IT, GlobalLogic

AN EMERGING TECH THAT'LL HAVE MASSIVE IMPACT IN 2019

Artificial Intelligence (AI)

MY FAVORITE SPORTSPERSON

Steve Waugh

MY FAVORITE POLITICIAN

Barack Obama

MY FAVORITE CUISINE

Thai

A TECH SHOW I FOLLOW

Global Security Exchange

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

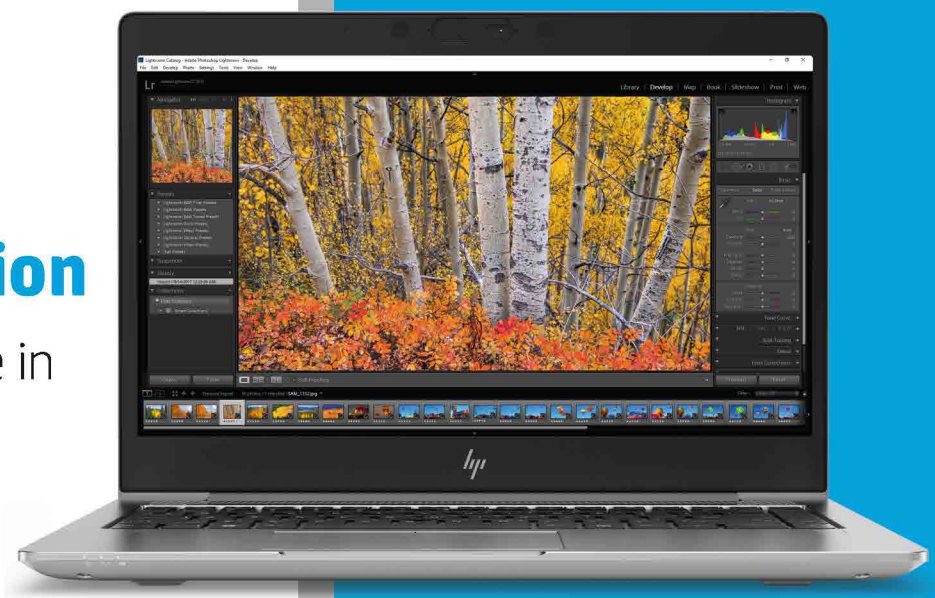
www.digit.in/hi
www.facebook.com/digithindi

डिजिट

miniTEK

HP ZBook 14u G5 Mobile Workstation

Remarkable performance in a thin and light design!



HP Zbook 14u G5

- Be productive in any situation
- Work with professional, certified discrete graphics
- Work at the speed of your ideas with the premium performance

HP Z4 Workstation

Perfect for engineering, visualization and Machine Learning!

Minitek Systems-Headquartered in Nasik, incepted in 1995 as IT Organization has our branch offices in Pune, Aurangabad & Mumbai. We provide Sales, Services and Information Technology Solutions under Consult - Design - Build - Operate - Maintain value chain covering the entire IT Infrastructure of an enterprise requirement. We have been honoured with HP Business Partners since 2005 and are HP GOLD Partners since 2012.

Contact Us

Sayali Desari: +91 9373 2415 08 | Nilisha Yadav: +91 9370 8967 35

Minitek Systems (India) Pvt. Ltd., Office No. 303, 2nd Floor, "Venture", Bhusari Colony, Paud Road, Kothrud, Pune - 411038.
Contact No.: +91- 20 - 25282015