

Insight | Pg 24

Exploring The Next Wave Of
Blockchain Innovation

Insight | Pg 30

Automation Is Becoming
A C-Suite Priority

IT NEX T

FOR THE NEXT GENERATION OF CIOs

CHIEF INTEGRATION OFFICER!

More technology dependence and cloud model mean business managers are taking tactical technology decisions independent of corporate IT. The role of IT leaders will increasingly be to integrate these tactical solutions meaningfully to maximize value for the enterprise.

**For NexGen IT leaders, the time
to get ready is now.**

LAUNCHING



Here is your chance to become a Digit certified tech influencer

Benefits of Digit Squad Member



Launch your own tech channel on Digit.in



Become a Digit Certified tech influencer

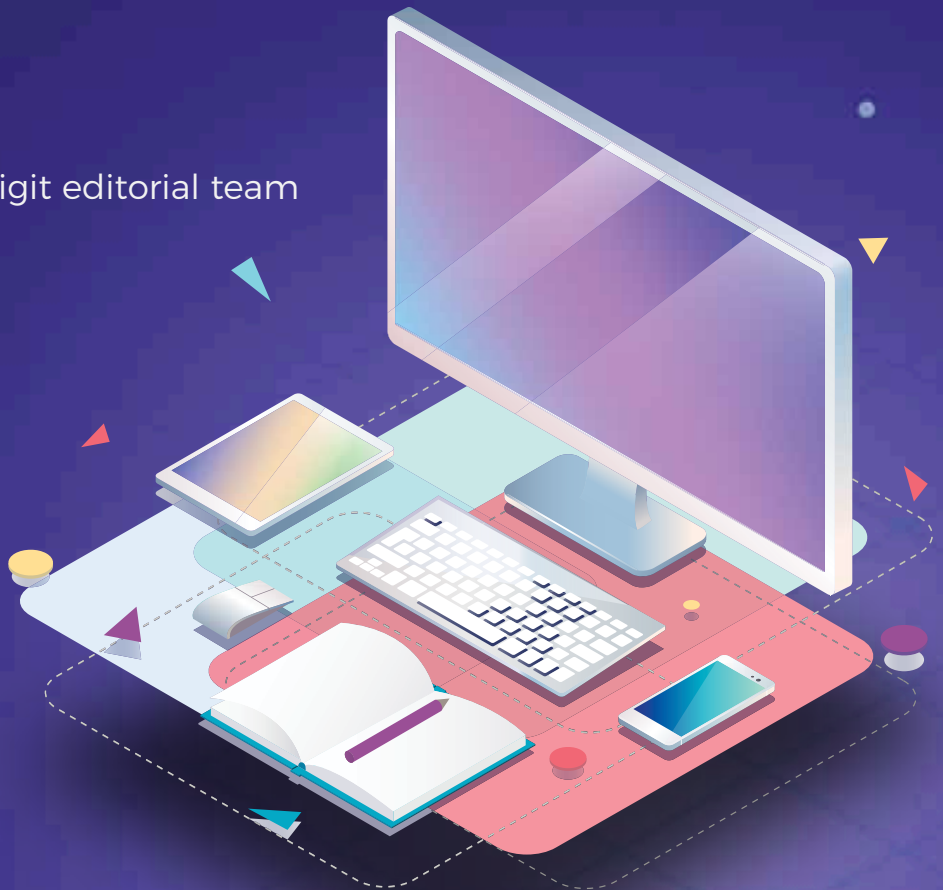


Engage with digit editorial team



Make money

Apply now by scanning the QR code



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

Are you a controller or value creator?



“Mature organizations do recognize that the value of technology comes most from combining the more efficient, more effective IT-leveraged parts of the business to create a whole organizational effectiveness that is more than the sum of the parts”

Shyamanuja Das

Most of the CIOs—irrespective of their age and experience—today realize that understanding of business and being able to communicate in the language business understands are extremely critical for carrying out their responsibilities as CIOs or senior IT managers.

However, those are at best, necessary conditions—and far from adequate to be an effective CIO.

This is why.

While most IT managers would talk to you about how CIO's role is changing and how the expectations from the CIO are changing, many are yet to reconcile to the fact that a CIO's importance in an organization is not measured (anymore) by the amount of budget he/she controls but the kind of business value he/she creates.

As the cover story in this issue illustrates, increasingly a lot of decisions concerning IT are being taken by the functional and LOB managers. Two factors have necessitated this change. On one hand, IT is now more interwoven in business; on the other, today cloud model allows the business managers to go for the functionalities that they are interested in without worrying about what lies beneath—the IT infrastructure.

Mature organizations do recognize that the value of technology comes most from combining the more efficient, more effective IT-leveraged parts of the business to create a whole organizational effectiveness that is more than the sum of the parts. In short, what the CEO/COO have been doing all these years, has to be supported by an effective technology and the person they turn to do that is the CIO.

That is why Sohini, who has written the cover story, calls them the Chief Integration Officers. They will increasingly help in maximizing business value through effective integration.

It requires a change in attitude—not change in skills. While among the older generation of CIOs it is considered a great virtue to be able to do that, it is becoming a basic expectation from the next generation.

That is why it is important that the next-level managers prepare themselves for the change. There's no certification for this. You just have to realign your expectations and tune your attitude.

Begin by unlinking your importance in your organization from the budget you control—even when the vendors who you deal with in your day-to-day life will try their best to make you believe the opposite. ■

Content

CHIEF INTEGRATION OFFICER!

More technology dependence and cloud model mean business managers are taking tactical technology decisions independent of corporate IT. The role of IT leaders will increasingly be to integrate these tactical solutions meaningfully to maximize value for the enterprise.

For NexGen IT leaders, the time to get ready is now.

■ COVER STORY | PAGE 08

FOR THE LATEST
TECHNOLOGY
UPDATES GO TO **ITNEXT.IN**

 **FACEBOOK**
[WWW.FACEBOOK.COM/ITNEXT99](http://www.facebook.com/ITNEXT99)

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

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



■ INTERVIEW | PAGE 14-15
"Future CIOs Should Prepare For A Journey Full Of Paradoxes"



■ INSIGHT | PAGE 16-17
How CIOs And Digital Leaders Can Reduce Consumer Trust Gap



■ INSIGHT | PAGE 28-29
AI For Fraud Detection To Triple By 2021, Says Study



■ INSIGHT | PAGE 32-33
Rise In Unauthorized Access Incidents A Key Concern For Customers: C-Suite Survey



■ INSIGHT | PAGE 36-37
IT-Based Attacks Increasingly Impacting OT Systems: Study



Cover Design:
BAIJU NV



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

SALES & MARKETING

Director - Community Engagement:
 Mahantesh Godi (+91 98804 36623)
Brand Head: Vandana Chauhan (+91 99589 84581)
Head - Community Engagement:
 Vivek Pandey (+91 9871498703)
Community Manager - B2B Tech: Megha Bhardwaj
Community Manager - B2B Tech: Renuka Deopa

Regional Sales Managers

North: Deepak Sharma (+91 98117 91110)
South: BN Raghavendra (+91 98453 81683)
West: Shankar Adaviyar (+91 9323998881)

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: 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



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

EXTRA Curricular



For the love of mountains and the joy of trekking

Trek On...

NEXT100 Winner 2016 **Kamalkishore Purohit**, Manager - IT, Mahindra & Mahindra shares his love for trekking and outlines his various adventures...

"Prioritize your passion. It keeps you sane."

I have always loved mountains and trekking brings me joy and enriches my life. It relaxes me and provides me pleasure because it is something which is not associated with daily responsibilities. It fills me with positive energy. It helps me to take my mind off the stresses of everyday life.

Durga Tekdi is a hill in Nigdi, Pune. It is visited by residents of Nigdi. The tekdi derives its name from the Durga temple on the hill. Durga Tekdi, also known as "Durgadevi Park" has always attracted me from my childhood days. Being a resident of Nigdi I have climbed this with my parents and then with friends from a very early age. Gradually, I started realizing that climbing this small hill up and down used to exhilarate and fill me with thrill and excitement.

My native place is Sikar in Rajasthan and we used to go there during summer and Christmas vacation. A part of Aravalli mountain range is spread in Sikar and there is a famous Harshanath temple of Lord Shiva on Harsha ki Pahari. I have never missed a chance to trek this small hillock whenever I was in Rajasthan.

As a teenager, I started satiating my enduring passion for adventure by climbing the famous Sinhagad Fort in Pune which is quite challenging and demands energy, stamina and enthusiasm.

During my college days, I got an opportunity to climb the Kalsubai Peak which is famous as the highest peak in Maharashtra. It lies in the Sahyadri Mountain range falling under Kalsubai Harishchandragad Wildlife Sanctuary.

Recently, I got a chance to go on Kheerganga and Bunbuni Pass trek from Kasol, which is among the most famous hill stations in the Pin Parvati Valley, one of the most scenic places in the Himalayan region of Himachal Pradesh.

While the incentives for trekking usually include testing one's physical strengths and resolution, the experience in itself is so much more. ■

As told to Dipanjan Mitra, Team ITNEXT



Kamalkishore Purohit

Kamalkishore Purohit is NEXT100 Winner 2016. He is Manager – IT at Mahindra & Mahindra. He has done his MBA in Production Operation & IB from

BAMU, Aurangabad, Masters in Computer Management from IMCD, Pune and Bachelor of Science (Electronics) from N. M. Wadia, Pune University.

Snapshot

Striking The Right Tune...

NEXT100 Winner 2014 **Makarand Joshi**, Head - IT Infrastructure, Endurance Technologies, shares his love for music. He illustrates the musical instruments he plays and mentions his favorite musicians...

It may not be exaggeration if I say “music is my soul”. Music is a stress releaser for me. Music brings tears to my eyes, spirituality to my mind and feeling of “Adwaita” with God. Listening a piece of classical “Khyal” after a hectic and stressful day at office while driving back home is blissful meditation.

Music is in our family and I have inherited it. My father was a flute player; my uncle was a well-known tabla player and another uncle was a vocalist. My memories of music go back to my childhood when I was around eight–nine years old. My elder sister and father used to play harmonium and do *riaz* (practice) of various Indian classical *ragas* and my father played the various *ragas* on his flute in the evening. I used to listen to those sweet melodies and it carved a deep love and passion in me for music.

I love Indian classical music the most. I listen to great artists, such as Pt. Bhimsen Joshi, Ustad Amir Khan, Pt. D.V. Paluskar, Kishori Amonkar, Pt. Ravi Shankar, Pt. Nikhil Banerjee, Ustad Zakir Hussain, Pt. Gajananbuwa Joshi, Pt. Kumar Gandharv and the list goes on. It is very difficult to name a few *Ragas* that I like. Some of my favourites “are *Yaman, Miya Malhaar, Malkauns, Bhimpalas, Durga, Hansdhwani, Madhuvanti, Miya ki Todi, Bhup, Bageshri, Abhogi* and many more.

Although I love Indian classical music, I am a keen listener of other forms of music also. I listen to Hindi and Marathi (my mother tongue) film songs, *ghazals* of Begam Akhtar, Gulam Ali and Mehdi Hassan. My favourite singers are Lata Mangeshkar, Mohammad Rafi, Talat Mahmood, K.L Saigal, Mukesh, Kishore Kumar, Geeta Dutt, Asha Bhosle and Hemant Kumar. I am also listen to Western classical and other music, especially symphonies of Mozart, Bach and Beethoven and groups like Boney M.



Music, the food for soul

The first musical instrument which I played was a set of bongo drums. It was gifted by my father when I was 11. He saw my love and skill playing different rhythms. Playing drums is my hobby and I play them whenever I get time from hectic professional life.

Later, I also purchased Conga drums and practice it in free time. Congas are used in both popular and folk music. African music has a varied use of Congas. This instrument is also very popular in Rumba, Afro Caribbean, Latin and Salsa music. It is idely used in Bollywood film songs.

In Indian tradition, it is assumed that there are 64 art forms and music is the closest art to Mother Nature, God and human soul. It is the best medicine to reduce your stress, bring calmness and peace to your mind and clarity and focus in your thoughts. Music is another form of meditation. ■

As told to Dipanjan Mitra, Team ITNEXT



Makarand Joshi

Makarand Joshi is NEXT100 Winner 2014. He is Head - IT Infrastructure, Endurance Technologies. Earlier, he was Head - IT Operations Excellence at Tata Technologies where

he served in managerial and leadership roles. He is an MCA from Pune University and Executive MBA from Symbiosis Institute of Business Management, Pune.

Snapshot



20TH CIO&LEADER CONFERENCE

CIOreLOADED

POWERING THE **NEXT** TRANSFORMATION

AUGUST 2ND - AUGUST 3RD 2019 | THE WESTIN GURGAON, NEW DELHI

POWERED BY



#CIOreLOADED

Customer Experience Partner



Gold Partners



servicenow

AI and Analytics Partner



Silver Partner



Associate Partner



Organised by



A Brand of



RSVP

For Sponsorship:

Mahantesh Godi
mahantesh.g@9dot9.in

For General Queries:

Renuka Deopa
renuka.deopa@9dot9.in

WHAT THE CIOs SAID IN 2018



"The content & the program was really enriching and its a great platform for meeting technology evangelists"

Gyan Pandey
Aurobindo Pharma

"This time the quality of speakers and their content was one notch up"

Abhishek Gupta
Dish TV



"Indeed a unique combination of fun learning combined with networking"

Parmeswar Menon
SBI Life Insurance Co



"The Deep dive workshops were unique and I appreciate the case studies"

Vipul Anand
Hindustan Sanitaryware &
Industries (HSIL)



CHIEF INTEGRATION OFFICER!

More technology dependence and cloud model mean business managers are taking tactical technology decisions independent of corporate IT. The role of IT leaders will increasingly be to integrate these tactical solutions meaningfully to maximize value for the enterprise.

For NexGen IT leaders, the time to get ready is now.



The changing tech decision equation calls for a drastic change in the mindset of the CIO. The time to plough the lonely furrow is definitely over. To succeed in this new scenario, the CIO must have strong collaborations with the C-suite.

By Sohini Bagchi

Today's enterprise IT managers know very well that it is critical to understand business expectations and the language of business to be able to effectively carry out their responsibilities. Ask any CIO or next-level IT manager about how the CIO's role is changing, and the answer you are most likely to get would have a heavy dose of understanding business needs, dynamics of business, language of business, business alignment, partnering with business and so on.

The fact is: Today's new enterprise IT professionals are not just aware of these needs but are more than convinced about their need to move beyond technology and understand business.

But just when the idea was sinking in and the IT leaders were beginning to find their new 'well-defined' role, it got disrupted again. This time, it was to do with their home turf – technology.

A few years back, Gartner came out with a sensational statement that

Chief Marketing Officers would soon spend more than CIOs on IT. That was a futuristic assessment based on forecasts, which some took seriously and some did not. But three years back, in 2016, the research firm came with a far more definite statement, quoting actual spend data to suggest that, indeed CMOs would spend more than CIOs on technology by 2017.

Of course, as it has been clarified now, the spend Gartner was referring to was what it called business IT—that excludes the large spends on infrastructure. But even then, it was quite disruptive as a news.

But Gartner's forecast about CMOs tech spending is not an isolated observation.

Changing Tech Decision Equation

Four trends have changed the technology decision-making equation in enterprises. These phenomena are only too familiar to us.

First is what is called consumerization of technology—more aware users

demanding what they want in terms of devices and applications. They were no longer willing to comply by everything that the corporate IT 'thrusts upon' them. But in isolation, this trend was initially restricted to mostly end-user devices and front-end applications. In any case, that was not the prime worry for CIOs in organizations with a more mature IT.

The second big driver was large-scale adoption of cloud—especially SaaS—which provided a far bigger disruption. It is not that business users did not want specific applications earlier. But to get that, they had to ensure that the infrastructure is in place. The business managers neither had the wherewithal to manage that IT infra nor had the authority to take capital expenditure decisions.

necessitated a need for Chief Digital Officers. Initially, CIOs and CMOs got into almost a duel on who was a better fit to take that position. But today, in hindsight, one can easily say that it is neither the CMO and CIOs but the core business managers who dominate the CDO landscape. Even organizations that did not have a designated CDO gave a lot of technology decisions formally to the businesses, so interwoven was technology now with business!

So far, this had impacted largely the services components of a business—sales, marketing, line businesses, HR, finance, customer service and so on. In 2016, World Economic Forum (WEF) Founder, Klaus Schwab, pronounced the arrival of the Fourth Industrial Revolution—it was all about digitization of manufacturing, leveraging emerging technologies like IoT. Every piece of

manufacturing equipment was now more and more digital. This was the fourth big trend.

To be fair, this was never a CIO's area. But with more IT going in, the expectation was that enterprise IT would have a role in managing some of it. Thanks to the completely different dynamics in which manufacturing OEMs operate, corporate IT, by and large is out of it.

All these changes did a few things to CIO's role.

One, it shrunk the IT budget that corporate IT handled. Cloud only accelerated that.

Two, it further aligned corporate IT from business IT—the more transformational IT, going by Gartner's bimodal IT classification.


However, it never freed the CIO from these responsibilities. CIO was still the go-to man (okay, woman too)

for anything that did not go right. Security and compliance were becoming big issues. Cyber security risk is one of the top five risks in the world today, according to WEF.

Also, as organizations started to think of complete transformation, those that did not have a full-time CDO—and such organizations were large in number—expected that the CIOs would provide a path. At least, CIO was the first person with which the top management started that discussion.

The CIO is now expected to play a more important role in organizational transformation. At the same time, his control over budgets and technology decisions was most definitely on the wane.

It is time for transformation for the CIO's mind. One of the things that is immediately required is to manage the changing situation in enterprise. And that is by collaborating well with the other business managers.



SaaS changed all that. It turned the purchase to a pure opex purchase. All functional/LOB managers were empowered to make those purchases. And they did not have to worry about managing the underlying tech...

SaaS changed all that. It turned the purchase to a pure opex purchase. All functional/LOB managers were empowered to make those purchases. And they did not have to worry about managing the underlying tech, which was done by the service provider.

That was a big power shift. While some of the big purchase decisions found roadblocks when there was need to connect them to enterprise IT systems—in order to extract their true value—many of the tactical point solutions continued to be purchased by the LOB managers. Corporate IT got bypassed for many such decisions.

While this changed the equation quite in favor of line managers, it still was not big enough as most large purchases were still going through corporate IT.

The third lever was the wave of digital transformation. Many businesses wanted to transform themselves, moving beyond just incremental efficiency enhancements. This

The Collaboration Imperative

To succeed in this new role, the CIO needs to have a strong collaboration with other C-suite members (CFO, CMO, CISOs, COO) as well as with heads of operational technology (OT) and line of business managers. For example, in today's customer-centric economy, CMO and CIO must collaborate and push their business forward, rather than work independently. As Kathleen Schaub, IDC Vice President - Research & CMO - Advisory Service, mentions, "No CMO today can be a good marketer unless they become a good technologist."

Today's marketers are harnessing the power of technology to reach out to potential prospects, increase brand awareness, and market new products. It is predicted that by 2025, the overall spend will grow to 10% of the USD 1.2 trillion total marketing spend compared to just 1% today, which is a colossal jump.

The changes are also becoming clearly visible. From companies implementing Customer Relationship Management (CRM) software to use of marketing automation software and digital marketing tools, marketers are constantly engaging consumers in new and innovative ways on various digital platforms. The interpretation of statistics, insights and intricate silos of data are essential in today's fast-paced digital world is bringing marketing and IT together, shows a new IBM survey, which mentions, one

of today's top priorities is to inject data-driven insights into every marketing decision.

The use of technologies, such as augmented reality and virtual reality, sensors, real-time social listening and several such tech-based marketing decisions are further making the CMO and the CIO collaboration even more potent.

Another very important relationship in the C-suite is IT's alignment with finance, which is often seen as siloed and disjointed. Several studies have shown CFOs often do not "speak the same language" with their CIOs and IT peers and they struggle to aggregate data across siloed systems beyond their direct financial management tools. As a recent research shows that part of the problem again is incompatible team cultures that are likely to hinder understanding and communication.

Successful organizations have managed to bridge the gap between the two roles. As Deloitte Consulting's Principal, Matt Schwenderman observes, "The CFOs that I consider being progressive and innovative, look to the CIO for ways to improve their own function, and are using the CIO to bring knowledge and skills that can be leveraged by finance."

CFOs are increasingly valuing the potential that CIO and his IT team brings, in the form of enhanced data analytics and technology adoption, just as CIOs need to develop greater influencing skills in order to deliver the change their business requires, believes Sunny Gupta, CEO at Apptio.

He opines, "CIO and CFO need to accelerate new delivery models, such as AI, cloud and agile, optimize technology spend to fund new innovation, and boost financial agility to make resource decisions that are aligned with the speed of business."

A close working relationship between leaders in IT and operational technology (OT) is being driven by digitalization. It is an important factor for improving the trust and confidence of supply chain partners.

Another very important relationship in the C-suite is IT's alignment with finance, which is often seen as siloed and disjointed. Several studies have shown CFOs often do not "speak the same language" with their CIOs and IT peers...

While digitalization demands convergence, a report by the Ponemon Institute released in February 2019 shows, executives often see convergence as a challenge that cannot be achieved without support from the company's CIO and other C-level executives.

Conflicts created by turf and silo issues are also significant organizational barriers to successful convergence. In this context, the creation of a cross-functional team to manage cyber risk across IT and OT systems will help eliminate this problem. A good understanding of third-party risk management, compliance with regulations and standards, and privacy program management can be a game changer, suggest experts.

Another change accompanying digital transformation is the shift in technology spending from IT to the Line of Business (LOB). A 2018 IDC forecast emphasizes that technology spending by line of business decision makers will overtake technology spending by the IT department by 2019-end. Roughly half of that spending will come from the IT budget


and so allows CIOs to focus more on the strategic needs of the business.

In practice, this means spending more time with LOB managers and with C-level executives, and less time overseeing operational matters.

Chris McGugan, a senior manager with Avaya, believes that the problem that exists is, while IT is focused on siloed technology developments, LOB is working to drive company-wide modernization. "Companies cannot have a siloed approach. Collaboration must increase between IT and LOB, whether that means IT having more involvement in LOB technology purchases or CIOs being more consultative to understand the problems that different business units face," mentions McGugan in her official blog.

The Way Forward

Collaboration is the starting point for next-generation IT managers, which helps them in understanding not just needs from an external perspective but the way these functional managers think.



Conflicts created by turf and silo issues are also significant organizational barriers to successful convergence. In this context, the creation of a cross-functional team to manage cyber risk across IT and OT systems will help...

while the other half will come from technology buyers outside of IT funded by LOB buyers and "shadow IT" without IT involvement.

Eileen Smith, Program Director -


Customer Insights & Analysis believes that cloud technologies, especially, SaaS, have been a key enabler for this transition. LOB managers are going for cloud based services, to deliver new services (because of speed and convenience), whether or not they are officially sanctioned by the IT department.

Cloud services will continue to play a large part in making the CIO more efficient. Cloud computing also brings standardization of functions and services, which in turn enables automation and in turn, less time and more productivity. For example, outsourcing infrastructure maintenance and operations to the cloud frees up time,

But what exactly is the CIO role evolving into? The jury is still out on that one but here are some pointers:

1. As organizations go for technology-leveraged strategic transformation, they expect technology to help them maximize business value, as an organization. This is different from better decision-making or operational efficiency or a specific new capability at a functional level. The whole value accrued to the organization must be more than the sum of parts. Someone needs to drive that.

That someone, for a very few selected organizations, is a dedicated Chief Digital Officer. But more than 95% of organizations do not have a CDO role; most of them do not intend to have one. Yet, they still need someone to put all the pieces together to create organizational value. That integration has to be done by someone who thoroughly understands technology and its direction as



Since collaboration is becoming a must in any major transformational exercise, just understanding business needs is not enough. Successful IT managers of tomorrow must be great in relationships and leveraging those relationships

well as business. In most organizations, CIO is the best person to drive that role.

The reason why it has not happened so widely is not as much because the top management has doubt over CIOs' capability as it is because the CIOs are not ready to move on from nuts and bolts because that may mean giving up control over a big chunk of budget on IT infrastructure. The moment IT leaders are ready to let that go, they will present themselves as the best available—if not perfect—candidate for this new integration role. So, are CIOs ready to be Chief Integration Officers?

2. Governance is becoming a major requirement at large companies. It requires a complete visibility as well as technology understanding today to be able to ensure effective governance. This is another role that CIOs are naturally suited to take up.
3. However, the most important CIO role is in helping to decide on and roll out technology for the organization's strategic goals and priorities. Today, technology impacts all the three planes—product, process and strategy. The individual business units mostly decide on the product-process related technologies. The organizational strategy—such as leveraging data or switching to platform model or helping create organizational

ecosystem (not any subcomponent of it) are still the work of CEO's office. These changes need to leverage the emerging technology today. That is a role only an enterprise-level technology manager can play. No marks for guessing who that is.

NexGen Managers: Are You Ready?

It is clear that the next-generation IT leaders who are likely to take over as CIO in the next 2-5 years need to be well prepared to take up this new expectation from the CIOs.

While today's IT managers are well-aware of the need to upgrade their skills, the big change required here is in attitude, not skills.

Here are a few specific changes required:

- a. They must start thinking themselves as strategic value creators than drawing their power from big budget and control.
 - b. Since collaboration is becoming a must in any major transformational exercise, just understanding business needs is not enough. Successful IT managers of tomorrow must be great in relationships and leveraging those relationships.
 - c. They should try to look at things from an external perspective—an outside-in view. Only that will help them find disruptive changes that can add significant value to business. Internal-focused business need understanding, however strong it is, can only create solutions for already created problem. It cannot pre-empt a challenge.
 - d. Governance is one area that every IT leaders should thoroughly understand.
 - e. Finally, every IT leader should figure out how to integrate. The integration skills will be their survival skills tomorrow.
- In short, the tech to business transformation of CIO is necessary, not sufficient. A good CIO must be able to work with everyone and integrate to create value that is more than sum of parts of the values brought in by technology to individual units.

It is becoming a core strategic role. But they have to give up what gives them a false sense of power—large technology purchase decisions. ■



“Future CIOs Should Prepare For A Journey Full Of Paradoxes”

In a conversation with CIO&Leader, **Mushtaq Ahmad, SVP and Chief Information Officer at CSS Corp**—one of the rare cases of a frontline business executive taking over as CIO—explains how the role is changing, the challenges in the industry and the technologies that he has invested in

By Sohini Bagchi

Q What foreseeable change do you see in the CIO role in the next 2-3 years?

A I believe, in the last couple of years, a CIO's role has transformed from a support function to a more complex and agile, core business function. The role will become even more multi-dimensional and challenging on all fronts. CIOs will be working more closely with other business functions across all levels of the organization to innovate on smarter technologies and identify newer ways to create impactful business outcomes. With technology being at the core of all new age organizations, more CIOs are likely to secure a place in the boardroom. A CIO will also hold more important responsibilities in data management functions going forward.

Q What are some of the key tech trends you foresee in the IT industry?

A Adoption of emerging technologies will continue to exponentially grow in the future. This includes cognitive technologies, such as open stack, artificial intelligence and machine learning. I strongly believe that these trends will fuel newer possibilities in specific areas like ambient computing and augmented reality. From an economic infrastructure point of view, 5G, cloud and SDX are likely to be the key trends that will open endless opportunities for organizations to bring their innovative ideas to life. In parallel, stackable technologies are also gaining more importance for its potential to supercharge the digitization efforts across organizations. Apart from this, there is also a keen focus on quantum computing. We will also see a shift towards an integrated automation approach. This approach will take intelligent automation, from desktop automation of disparate tasks, to the next level of business process transformation by effectively bringing together technology, talent, organizational change, and leadership.

Q What kind of technologies has your organization invested in recently? What technologies you intend to explore in the future?

A We have invested heavily into technology and continue to invest in the emerging and niche areas. At CSS Corp, we build outcome-based services using cognitive technologies to help organizations integrate our solutions into their environments in a hassle-free and risk-free way. In terms of advanced technology adoption, we are investing significantly in our innovation lab, where we have built over 25 digital solutions that accelerate technology adoption and drive business results. These solutions are implemented for our customers and have yielded great results.

We are also evolving our cognitive customer experience suite to not only transform the customer experience but also drive system efficiency and boost engineer experience. By leveraging AI technology, we aim to augment agents' experience in contact centers and improve their productivity. On the other hand, we are constantly upgrading our cognitive analytics capabilities with emerging data sources and platforms.

Additionally, we have built a robust intelligent automation suite for monitoring and managing IT operations for our customers. Another area of focus for us is advanced location analytics and insights, which have become essential for organizations to provide personalized services to their customers.

Q What are some of the biggest challenges you face, in your industry?

A A key challenge we face lies at two extremes of a spectrum—either it's lack of trust in technology to deliver any results or expecting technology to be the magic bullet to all problems. To overcome this, we spend ample time to understand our customer's apprehensions and business objectives, and work with

“Leaders of tomorrow should build effective partnerships that are outcome-based, revenue generating and customer-centric”

them to craft a pragmatic solution that delivers on the promise.

The other challenge is more tangible in nature. The exponential growth of digitalization has posed huge cybersecurity threats like phishing, DDoS attacks, crypto mining and botnets. It is becoming a challenge for CIOs to keep organizations safe with teams lacking specialized cybersecurity professionals and the ever-increasing cyber incidents gathering under their belt every year.

Data privacy regulations and end-user awareness is another critical area. We need to understand that IT alone cannot solve all problems through technology adoption. With technology improving and catching up with bad actor techniques, the focus is shifting towards exploiting the end-users to collect information. Therefore, end-user awareness, mandatory certifications about various regulations and social engineering techniques are crucial to secure data storage and transaction.

Q What's your digital agenda? Do you find the right talent to meet your organization's digital needs?

A Our digital agenda is a convergent approach. We strive to hire professionals with the right attitude apart from the digital know how. Since technology and various stacks are getting converged, there is a greater need for various skills to be combined accordingly as well. This is the shift and the demand we are receiving today

from the market. Therefore, we are investing deeply in technology training, upskilling and infusing emerging technologies/skills to our employees.

A continuous learning mind-set, hunger and passion can help employees scale-up to meet the requirements in hand. We have also built high value learning and development frameworks that facilitates faster on-boarding and better understanding of technologies, customer products and environments. An engineer joining our customer experience team today, can resolve issues 2-3 times faster when compared to his/her resolution rate few years ago. This is largely due to their increased aptitude to understand applicability of emerging technologies and AI in support processes, and application of knowledge management in business operations. In some of the recent engagements, our AI solutions have decreased the new-hire learning from 90 days to 25-30 days.

Q What is your advice for future technology leaders?

A Future technology leaders and CIOs should prepare for a journey full of paradoxes, with steep and sky-high targets with limited means to achieve them. CIOs and technology leaders should lead technology strategy and adoption by being a transformation and change agent.

I would advise new-age technology leaders to constantly invest in themselves and their peers when it comes to continual learning and upgrading skills. Leaders of tomorrow should also build effective partnerships that are outcome-based, revenue generating and customer-centric. They should learn the art of getting into consulting or advisory roles as organizations will increasingly rely on them to guide with their technology strategies.

Aspiring technologists should also be up-to-date with the latest and greatest trends in the technology world. They should be open to learn from different sources and invest in peer learning, while remaining agile and responsive to the demands of the market. ■



How CIOs And Digital Leaders Can Reduce Consumer Trust Gap

Organizations should focus on privacy, security and compliance when offering digital services to customers

By Sohini Bagchi

Trust is critical for organizations to succeed in this digital world as consumers overwhelmingly prefer to transact with a trusted digital platform. However, a new study jointly conducted by Microsoft and IDC reveals that only 41% consumers in India trust organizations that offer

digital services to protect their personal data. Experts believe that CIO/CTO and other digital leaders can play a credible role to reduce this trust gap.

The study conducted amongst 6,400 consumers and senior leaders across 14 markets in India asked respondents to provide their opinions on certain elements of trust, including: privacy,

security, reliability, ethics, and compliance – when using digital services.

The study revealed that consumers feel that all these elements of trust are almost equally important to them. Specifically, security (86%), privacy (85%) and compliance (82%) emerged as the top three most important elements. Consumers also have the high-

est expectations of trust from financial services institutions, followed by education institutions and retailers, finds the study.

Trusted platform, a priority

The study states that establishing a trusted platform needs to be a priority in organizations' strategy for digital services. Close to half of the consumers (46%) in India have had their trust compromised when using digital services.

More than half (51%) of the respondents indicated that they would switch to another organization and one-third of consumers would stop using the digital service altogether. Another interesting finding is that though Indian consumers are known to be price-sensitive, close to 73% consumers highlighted that they would recommend a trusted digital service to others even if the cost is higher.

"The upside for organizations with a trusted digital platform is tremendous as India is one of the largest and fastest growing digital services markets in Asia Pacific where almost all of the transactions and interactions would be digital in the near future," Keshav Dhakad, Group Head & Assistant General Counsel – Corporate, External & Legal Affairs, Microsoft India, opines.

Highlighting the need for CIO/CTO/CDO in digital services firms to address the trust gap, Dhakad says, "Most consumers still do not perceive organizations to be trusted data stewards. It is clear that businesses need to do a lot more to understand what drives consumer trust and focus on how they can build trust and make it a key competitive advantage for their digital services."

The study shows CIOs and digital leaders should focus on two things when they deal with consumer trust issues. One, trust should be the foundation of digital transformation plans and second, security and privacy are the two most important trust elements.

Using AI as a tool

The Microsoft-IDC study deduces

that technologies such as artificial intelligence (AI) can play a key role in reducing trust gap, and digital leaders including CIOs can establish a trusted framework in order to do so. Consumers in India have the highest trust in financial services institutions, education institutions and automotive companies to harness AI to improve their lives.

According to a study conducted by IBM's Institute for Business Value, in 2018, eight out of 10 high-performing enterprises are now considering or moving ahead with AI adoption. CIOs of those firms assert their organization's ability to drive revenues, improve customer service, lower costs, and manage risk. However, although they realize the huge benefits of this technology, 60% percent of those companies fear liability issues and an equal number say they lack the skills to harness AI's potential, according to the same study.

Italian computer scientist and professor, Francesca Rossi, who has done extensive research in artificial intelligence, writes in her blog, "Trust in the technology should be complemented by trust in those producing the technology. Yet such trust can only be gained if companies are transparent about their data usage policies and the design choices made while designing and developing new products."

She continues, "If data are needed to help AI make better decisions, it is important that the human providing the data is aware of how his/her data are handled, where they are stored, and how they are used."

Likewise, Dhakad believes, for the development and usage of AI and technology in general, we must first consider its impact on individuals, businesses and society.

Tech collaboration with government

Dialogue between technology companies and governments and also other industry stakeholders is necessary. Consumers in India feel that technology companies (46%) followed by governments (34%) should be responsible

for building trust, indicating the need for a stronger partnership between the private and public sector.

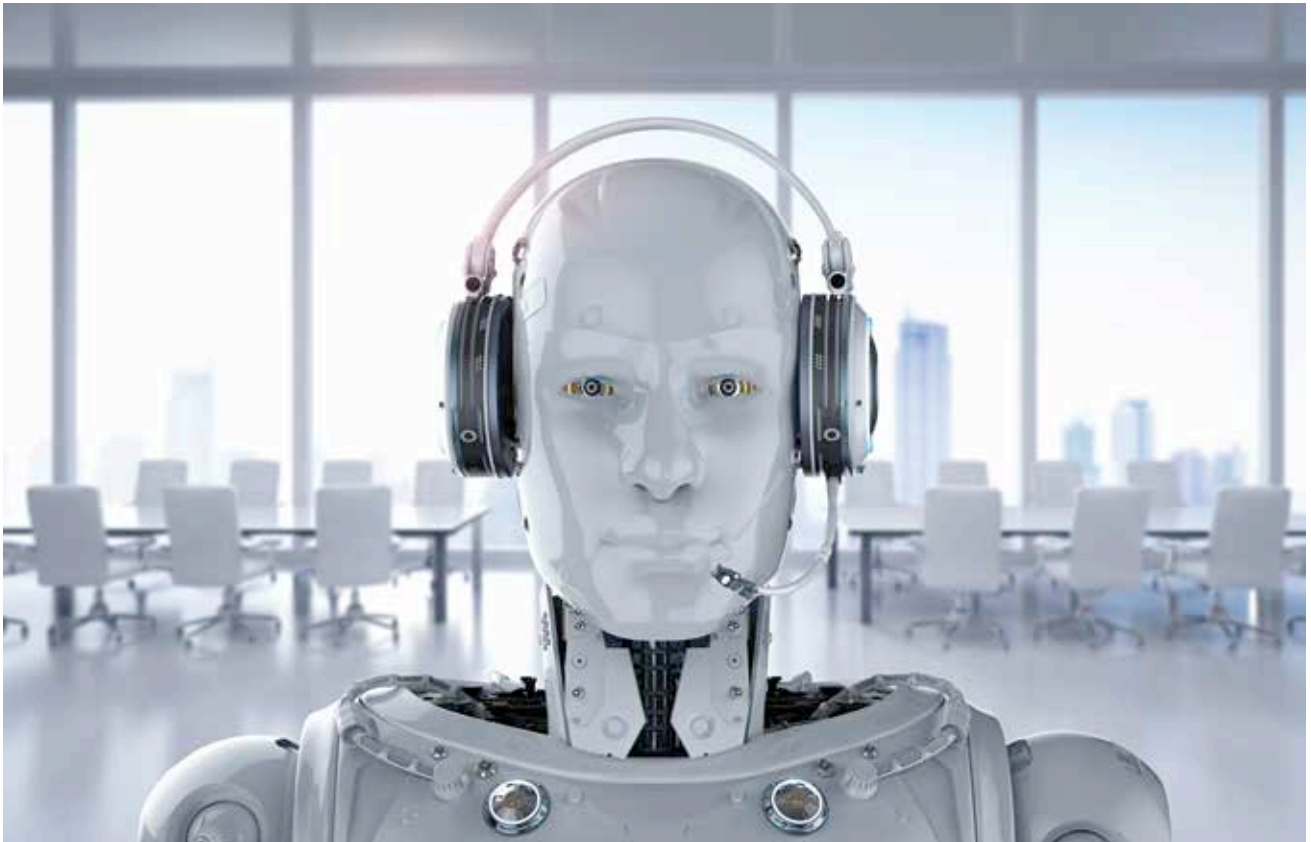
In other words, the study suggests that not just organizations providing digital services, but the broader industry, including institutions which set rules and regulations, should be responsible for building trust. It is through meaningful collaboration that digital leaders can build an ecosystem that values trust.

Regulations such as the General Data Protection Regulation (GDPR) in Europe and India's draft Data Protection Bill provide some fundamental rights over personal data. For instance, GDPR mentions, besides performance and accuracy, bias definition and detection and mitigation methods should also be communicated clearly and made accessible to all users.

Dhakad opines, "This would require a broader debate on ethics, policy and regulation that involves the appropriate stakeholders, including the government and technology companies. These dialogues would need to be backed by actions, including forging closer partnerships and facilitating greater knowledge exchange and industry best practices. These are all necessary steps that will enable us to collectively establish a well-balanced, holistic baseline for trust for the entire industry," he states.

"As most consumers still do not perceive organizations to be trusted data stewards, it is clear that CIOs and digital leaders need to do a lot more to understand what drives consumer trust and focus on how they can build trust and make it a key competitive advantage for their digital services," states Ranganath Sadasiva, Director – Enterprise Solutions, IDC India.

"As competition between digital services becomes more intense and global in nature, advocacy through word of mouth can be a strong differentiator for the organization and a shot in the arm for the brand," he says adding that only a holistic, multi-disciplinary, and multi-stakeholder approach can build such a system of trust. ■



Inducing 'Empathy' In AI Can Heighten Customer Experience

CIOs and technology leaders should institutionalize empathy with AI platform for heightened customer experience, says a new study

By Sohini Bagchi

Many businesses are turning to artificial intelligence (AI) such as digital assistants and chatbots to improve customer experience. However, a new report released by Pegasystems indicates that consumers lack an understanding of how they can benefit from AI tools and systems.

The research indicates that empathy is the key to AI-based interaction between

brand and its customer. It also demands that CIOs and technology leaders institutionalize empathy with AI platform for heightened customer experience.

Can AI replace real person

The study shows that despite the growing usage of AI technologies, consumers are more likely to trust a real person to help make decisions. Users trust only those AI tools that seek to incorporate empathy and

ethical-decision making, as Dr Rob Walker, vice president, decisioning and analytics at Pega, explains how empathy is the key ingredient of building trust between humans and technology.

“When it comes to seeking a personal loan from a bank, only 25% consumers (as per the study) trusted a decision made by an AI system,” he says, adding that at the same time, if a human expert intervenes on the regulatory processes before making the loan offer to an individual and does the follow up, it becomes more trustworthy.

“Consumers likely prefer speaking to people because they have a greater degree of trust in them and believe it’s possible to influence the decision, when that’s far from the case. What’s needed is the ability for AI systems to help companies make ethical decisions.”

Why firms should care?

The study highlights that there are serious trust issues with AI. Nearly half (40%) of respondents agreed that AI has the potential to improve the customer service of businesses they interact with. This is where firms got to care, as the lack of trust, as the research shows, can have a negative impact on the customer’s digital experience and ultimately, on brand’s reputation. Moreover, consumers are cynical about the companies they do business with, finds the study.

Researchers believe, when teams that are considering implementing AI, give customers the opportunity to choose whether they prefer an AI-based or human-driven experience to solve their inquiry – it turns out to be a step towards building trust and transparency.

Despite this, 65% of respondents don’t trust that companies have their best interests at heart, raising significant questions about how much trust they have in the technology businesses use to interact with them. Many believe that AI is unable to make unbiased decisions: Over half (53%) of respondents said it’s possible for AI to show bias in the way it makes decisions.

People still prefer the human touch, with 70% of respondents still preferring to speak to a human than an AI system or a chatbot when dealing with customer service. Most believe that AI does not utilize morality or empathy. Over half (56%) of customers don’t believe it is possible to develop machines that behave morally. For example, assigning female genders to digital assistants such as Apple’s Siri and Amazon’s Alexa is helping entrench harmful gender biases, according to a new research released by UNESCO.

“Because the speech of most voice assistants is female, it sends a signal that women are obliging, docile and

instance in areas such as racial or gender discrimination.

CIOs will also need to think twice about giving too much decision-making authority to machines. They need to ensure that they understand and can explain the methods machines are using to make decisions. Some organizations for example, also have formed ethics committees to oversee questionable aspects of data use.

Another very effectively way CIOs can close the AI-customer gap is by embracing ‘design feeling.’ Design feeling aims to help developers focus on how their designs make users feel, rather than on seeing designs solely as a solution to a problem.

Companies need to be transparent about the data they use to train machine-learning algorithms to ensure that these algorithms don’t end up perpetuating racial or gender discrimination

eager-to-please helpers, available at the touch of a button or with a blunt voice command like ‘hey’ or ‘OK,’” the report said, adding that technology firms were “staffed by overwhelmingly male engineering teams” and that “the subservience of digital voice assistants becomes especially concerning when these machines give deflecting, lack-lustre or apologetic responses even to verbal sexual harassment.

AI demands new leadership from CIOs

The age of AI demands new leadership from CIOs – in the way they design, implement and regulate their AI strategies. Experts believe, in the coming years, CIOs will need to pay even closer attention to the potential for algorithmic bias in machine learning. Companies need to be transparent about the data they use to train machine-learning algorithms to ensure that these algorithms don’t end up perpetuating, for

Danielle Krettek, founder of the Empathy Research Lab at Google in her blog mentions that businesses need to start thinking about design feeling as the next iteration of design thinking, the now widely used methodology aimed at creating more innovative and “human-centered” design concepts. This is an area Google is focusing on in its innovation lab.

Similarly, with Pegasystems Customer Empathy Advisor, a new AI tool for optimal customer experience, CIOs can measure and calibrate the degree of empathy in customer interactions and improve user experience.

To ensure heightened customer engagement and experience, machines have to understand the humans that are using them. Soon there will be computers that can tell the difference between a smile and a smirk. Such level of sophistication can make their interactions with businesses better and more efficient, believe AI experts. ■



Data-Centric Security In The Era Of Data Protection And Privacy Journey

Data-centric security embeds controls into the data itself so that these controls are intact to the data even when the data is at rest or in motion or even while the data is being utilized in an application

By Prakash Kumar Ranjan

Data is key to any organization. Every organization has data which is vital for their organizational growth. Most organizations build security around structured data which is mostly stored in the database. But typically, more than 80% data are unstructured. Organizations need to

protect the data from unauthorized access not only from external users but also from internal users.

Data-centric security embeds controls into the data itself so that these controls are intact to the data even when the data is at rest or in motion or even while the data is being utilized in an application.

In data-centric security, data is independent of the security of the infrastructure, be it device, application, network or the method of transport of data. Data leaks not only put tarnish the reputation but also lead to penalties/legal action. The new regulations require organization to build control around security and privacy of the

data even if the data travels within the boundary of the organization or goes outside its boundary.

Basically, the core data-centric security solutions consist of the following:

1. Data Classification
2. Data Loss Prevention (DLP)
3. Cloud Access Security Broker (CASB)
4. Digital/Information Rights Management (IRM, DRM, ERM, EDRM)

Data Classification – Data classification is the process of identifying and labelling the information/data preferably on the sensitivity of the data. Most classification tools have an element of machine learning based on content and context. This increases the effectiveness of DLP, CASB, EDRM tools.

Data Loss Prevention (DLP) – DLP is a system that performs real-time scanning of data at rest and in motion, evaluates that data against existing policy definitions, identifies policy violations and automatically enforces some type of pre-defined remediation actions, such as alerting users and administrators, quarantining suspicious files, encrypting data or blocking traffic outright.

Cloud Access Security Broker (CASB) – CASB helps in identifying, monitoring and controlling the enterprise data in Cloud Infrastructure and it extends control to the Cloud applications. It is also sometimes referred as Cloud DLP in terms of data-centric security.

Digital/Information Rights Management (IRM, DRM, ERM, EDRM) – DRM embeds the security controls into the data itself. These controls remain active even if data is being used or worked and it also remains persistent during the movement of data.

It helps the enterprise to have control over the data even if the data has left the boundary of the enterprise. Some popular controls of DRM are self-destruction of data or disallowing copy/paste/print of the document.

Scenario of Data-centric Security

One of the directors of the enterprise is on leave and has no access to corpo-



rate emails or applications. An urgent Board Note (confidential document) needs to be vetted by him. Now the director asks his office to send email to his personal email with the Board Note for his views. His office sends him the Board Note to his personal email.

How can the security of the document be ensured?

Can we assume that after giving his views on the note, he has deleted the data from the device or email box?

Can the enterprise be 100% sure that data would not be misused in future? – NO

Solution – If we enforce DRM on the document, we can set the period of the life of the document itself. We can even recall or revoke access to information that we have shared with anybody. DRM maps the policy so that the document can be protected automatically whenever they are discovered, detected, downloaded or shared.

Emergence of Data Protection Laws

2018 has been a significant year for privacy and data protection laws in the world.

Some of the popular data protection laws are:

GDPR – The EU General Data Protection Regulation (GDPR) took effect on May 25, 2019 and is a regulation in EU law on data protection and pri-

vacy for all individuals/citizens of the European Union (EU) and the European Economic Area (EEA). GDPR aims primarily to give control to individuals over their personal data and simplifies the regulatory environment for international business by unifying the regulation within the EU.

CCPA – The California Consumer Privacy Act (CCPA) – a US law – got passed in California in 2018 and takes effect on January 1, 2020. The CCPA applies to businesses (regardless of location), which collect personal information about California residents, including customers and employees.

Bahrain has also passed a new, comprehensive data protection law making it the first Middle East country to adopt a comprehensive privacy law.

One of the most significant privacy law developments of 2019 is expected from India. India's draft bill introduces specific rights for individuals as well as requirements processing entities have to meet. For example, businesses will need to implement organizational and technical safeguards regarding the processing of personal data, including cross-border data transfers. The law also seeks establishment of a Data Protection Authority for overseeing data processing activities. ■

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



Business Email Compromise – When Defying An ‘Executive’ Is The Right Thing To Do

Organizations should consider using a multilayered identification process for transferring resources and invest in smart email protection

By Nilesh Jain

Email security is a top-of-mind concern for many organizations, with Business Email Compromise (BEC) gaining prominence as one of the lethal tactics adopted by cybercriminals to attack enterprises. Law enforcement agencies worldwide have been keeping a close watch on BEC scams as a result of the increasing losses year on year. According to

the Federal Bureau of Investigation (FBI), BEC has incurred nearly USD 12.5 billion losses to companies as of 2018. On average, one successful BEC attack can cost the company USD 130,000. We reported the number of BEC attacks in 2018 increased by 28% globally.

Falling victim to a BEC scam has long been a problem that generally arises from human negligence and our natural inclination to do

what someone in authority asks of us. Because these scams do not have any malicious links or attachments, they can evade traditional detections. These two factors make BEC a persistent threat for enterprises. Before we delve into what measures an enterprise need to take to mitigate risks associated with BEC, it is important to know how it works.

At the core of it, BEC is a form of spear phishing where an attacker, by pretending to be a high-ranking executive – usually the CEO, attempts to trick a victim – usually the CFO – into paying a fraudulent invoice. To do so, fraudsters carefully research and closely monitor the potential target victims – both the spooked executive and the one issuing the payment – and their organizations. The tone of the email is usually urgent.

It is also observed that most BEC attempts happen in countries with established business hubs and those that see a lot of multinational business operations.

BEC persists and new trends arise

In India, some 1.5 billion email threats were blocked in 2018. BEC, as a form of email-based scam, remains a very potent and lucrative means of funneling money from companies. As per our security predictions for 2019, BEC scammers will target employees further down the company hierarchy this year, for example, secretaries or executive assistants.

In what appears to be a product of masterful social engineering, BEC scammers are also reportedly using domestic money mules recruited via confidence or romance scams. After grooming these victims, scammers will trick them into opening accounts that will only be used for short term, presumably to avoid being tracked by the authorities. Another phenomenon noticed is that some BEC victims are tricked to purchase gift cards. In this BEC variation, a cybercriminal posing as a person in authority may send a spoofed

email, phone call, or text to a victim, requesting to buy gift cards for personal or business purposes.

Gearing up against BEC threats

Businesses are advised to stay vigilant and educate employees on how not to fall victim to BEC scams and other similar attacks. It's true that cybercriminals usually prefer big companies but there's little guarantee that small and medium-sized enterprises won't get hit. For one thing, smaller companies tend to have less robust security infrastructure in place.

details, and reasons behind payments.

- Confirm requests for transfer of funds when using phone verification as part of two-factor authentication, use known familiar numbers, not the details provided in the email requests.
- If you suspect that you have been targeted by a BEC email, report the incident immediately to law enforcement or file a complaint with the cybercrime department. Organizations should consider using a multilayered identification process for transferring resources and



Here are some tips on how to stay protected and secure:

- Be wary of irregular emails that are sent from C-suite executives authorizing an urgent payment. Look for discrepancies in the email address, the way it is written, the sign-off, and more. Review past emails that request transfer of funds to determine if this one is irregular.
- Cybersecurity awareness training and enforcing best practices against email threats can help employees stay alert and not fall prey to these attacks.
- Verify any changes in vendor payment details by using a secondary sign-off by company personnel.
- Stay updated on your customers and vendors' habits, including the

invest in smart email protection. There are advanced security technologies available now that can prevent users and organizations from falling for BEC attacks. For example, by studying and learning the unique ways executives compose their emails, a new AI-based technology is able to pick up on tiny details that set authentic emails apart from fraudulent ones, leading to better detection of BEC scams.

BEC is here to stay, with Gartner predicting that through 2023, business compromise attacks will be persistent and evasive, leading to large financial fraud losses for enterprises and data breaches for organizations. ■

The author is Vice President, South-East Asia & India, Trend Micro



Exploring The Next Wave Of Blockchain Innovation

Blockchain promises to disrupt many industries and not just the obvious ones like banking and financial services

By Karthik Ramarao

The first thing that comes to mind when we talk about blockchain, is Bitcoin. Blockchain has been stereotyped or correlated with Bitcoin and cryptocurrencies even though its applications lies far beyond, with high potential in auditing, healthcare, business and even cloud computing. The technology has come a long way since its inception and is now being adopted by enterprises for day-to-day functions like invoice automation, fraud control, patent tracking, etc. People

have realized that blockchain technology can be used in a myriad of ways and applications.

The global blockchain market is expected to be worth USD 20 Billion in 2024. Blockchain becomes the core enabling technology for financial institutions to move into the modern age of real time transactions. Government, medical and IT industries are all experimenting with the advanced blockchain solutions. Corporate can work with NGOs/ non-profit organizations to sustain a healthy and transparent way to give back

to society by creating a social good ecosystem. Holistic policies are used to create a paradigm shift in using blockchain technology for creating directional social impact.

By bringing digital technology into real time computing systems management, blockchain changes all aspects of our economy including healthcare, shopping, entertainment, education as well as social networks.

Blockchain new-age applications

Blockchain applications have been extracted from the use-case of Bitcoin to varied fields. It started off with banking and is slowly moving in to different fields.

1. Government

Blockchain empowers government to verify citizen's identity for legitimate voting. It facilitates government to store immutable citizen data with an extra level of protection to private data. With blockchain technology census enumeration can be made more accurate. Citizenship participation and crowd-funding ventures can also be revolutionized using blockchain technology.

2. Healthcare

Blockchain offers a secure, decentralized, and efficient solution for digital health records exchange and pharmaceutical supply chain management. Blockchain technology makes redundant the siloed nature of health records by compiling them in distributed ledgers. This interoperability allows doctors to view patient details which are otherwise scattered across many systems. This technology can be further leveraged for temperature monitoring and counterfeit drug prevention in pharmaceutical supply chains. All access control can be with the patient though.

3. Environment and energy

Blockchain technology helps to increase the efficiency of existing-grids as well as the peer-to-peer transac-

tion of energy and payments. It can increase trust and transparency in the carbon credit exchange and reward individuals who recycle as well as produce clean energy.

4. Agriculture

Farm to fork can be revolutionized with blockchain technology with improved transparency, traceability and efficiency in the entire supply chain from farmers to consumers. It can help to save revenue by bringing down food contamination and food fraud incidents by taking out the third party and improving supply chain tracking. The technology will ensure that farmers receive timely payment for their produce.

**By bringing
digital technology
into real time
computing systems
management,
blockchain changes
all aspects of our
economy including
healthcare,
shopping,
entertainment,
education as well as
social networks**

5. Philanthropy

Blockchain technology has caught the attention of Philanthropists as they are using it to bring in more transparency toward the rightful usage of their generous contributions. Blockchain also helps charitable organizations by enhancing transparency, reducing costs through disintermediation, and enabling new mechanisms for monitoring and tracking impact. It will

also provide emerging models for new sources of revenue and fundraising.

6. Digital identity

Blockchain based digital identity allows user-centric databases which allows individuals to have a complete control over who has access to their data. This will help to reduce fraud, increase transparency and efficiency.

7. Land rights

Blockchain technology brings in transparency to land registration process and allows storage and verification of titles and ownership. It reduces documentation-based fraud and paves way to improved information, efficient processes and transactions. Blockchain enabled smart contracts can make official processes like land registration much easier and save time and cost.

8. Education

Blockchain technology will help to reduce the administrative cost levied to verify and authenticate records as well as to provide a secure and immutable record of attendance and performance which can replace current methods of issuing certificates. It can enable a compiled portfolio of all student related information. Students can benefit from it by compiling their workbook into a distributed ledger that peers can benefit from.

9. Sanitation and water supply

Blockchain technology creates an efficient way to track and record water data as well as to create more efficient markets for natural resources that are being exploited.

Focusing on Blockchain's potential to reduce cost, increase efficiency, instill trust and improve security will enable this technology to move away from the hype and become a full-fledged technology enabler in all spheres of businesses in the coming days. ■

The author is Founder & CTO, Empirical Data



Are CIOs Losing The Cyber Security Battle?

Nine out of 10 CIOs in a recent survey believe staying up-to-date with cybersecurity technology is a challenge

CIOs and security teams spend a good number of their work hours managing security. Yet they are challenged with issues, such as a lack of expertise, budget and up-to-date technology. And as a result of which they are struggling to plug all the security gaps, according to a new report.

In a recent research report by Sophos, titled 'The Impossible Puzzle of Cyber-security', conducted through a survey by Vanson Bourne, researchers polled 3,100 IT managers across 12 countries including India. The respondents, mainly CIO, CISO and security professionals, who worked for organizations between

100 and 5,000 users, reported difficulties in protecting their infrastructures, leading to a large number of successful hacks.

IT low on expertise, budget and technology

As per the survey, globally, two out of three organizations (68%) suffered a cyber attack in 2018 that they were unable to prevent from entering their network. Nine out of 10 (91%) said they were running up-to-date cybersecurity protection at the time.

Coming specifically to Indian businesses, the survey, Indian CIOs and IT managers reported that 32% of their team's time is spent managing security, on average. Yet, only 8% believe they have strong team in place to detect, investigate and respond to security incidents.

"Staying on top of where threats are coming from takes dedicated expertise, but IT managers often have a hard time finding the right talent or don't have a proper security system in place that allows them to respond quickly and efficiently to attacks," says Chester Wisniewski, principal research scientist at Sophos.

Regarding budget, eight out of 10 respondents said their organization's cybersecurity budget (including people and technology) is below what it needs to be. Having current technology in place is another problem, with almost everyone agreeing that staying up-to-date with cybersecurity technology is a challenge for their organization.

This lack of security expertise, budget and up-to-date technology indicates IT managers are struggling to respond to cyberattacks instead of proactively planning and handling what's coming next.

Lesson for CIOs

Despite taking tangible steps to reduce their cybersecurity risk, a question that comes to mind is, 'Why are companies still getting hit and more than ever?' The report clarifies that there are some security holes not



With cyber threats coming from supply chain attacks, phishing emails, software exploits, vulnerabilities, insecure wireless networks, and much more, businesses need a security solution that helps them eliminate gaps and better identify previously unseen threats

being plugged and it is here that CIOs need to pay greater attention.

For example, the report explains, an up-to-date malware signature list won't stop attackers hijacking your accounts, while rock-solid authentication won't help if you're not protecting your computers from ransomware. "Good cybersecurity demands defense in depth and proper risk assessment so that you can protect your weakest spots from attack first," says the report.

The survey also revealed that companies are facing attacks via multiple channels, including email (33%) and web (30%) among others. Software vulnerabilities and unauthorized USB sticks or other external devices were also common attack vectors. Perhaps even more worrying is that 20% of CIOs didn't know how their networks were compromised.

With cyber threats coming from supply chain attacks, phishing emails, software exploits, vulnerabilities, insecure wireless networks, and much more, businesses need a security solution that helps them eliminate gaps and better identify previously unseen threats.

"If organizations can adopt a security system with products that work together to share intelligence and automatically react to threats, then IT security teams can avoid the trap of perpetually catching up after yesterday's attack and better defend against what's going to happen tomorrow," explains Wisniewski.

He believes that having a security 'system' in place helps alleviate the security skills gap CIOs are facing. "It's much more time and cost effective for businesses to grow their security maturity with simple to use tools that coordinate with each other across an entire estate," he concludes. ■



AI For Fraud Detection To Triple By 2021, Says Study

Soon more and more companies will invest in AI tools to combat cyber threats

Until recently, the enterprise segment has been slow to incorporate AI as a security measure – the obvious reason being AI itself is still a work in progress and it took a while for CIO/CISOs to cut through the noise and understand how it impacts business. But that's

going to change in the coming months, believe researchers.

A global survey by the Association of Certified Fraud Examiners (ACFE) reveals that while only 13% of organizations use AI and machine learning to detect and deter fraud, another 25% plan to adopt such technologies in the next year or two – a nearly 200%

increase in the use of AI to mitigate security risks.

The report that was developed in collaboration with analytics leader SAS and polls more than 1,000 executives on the use of technology to fight fraud mentions: "As cyber goons are becoming more adept at stealthily finding their way into computer

networks, the security industry has significantly stepped up its focus on AI and machine learning as a preventive measure against invasion.”

There are already some very successful use cases by businesses using AI to mitigate fraud. Walmart for example, is using AI technology to combat one of its key business challenges. The retail giant has deployed cameras with AI to reduce checkout theft in more than 1,000 stores across the US. The system is able to detect when an item goes un-scanned. It reports the error to a checkout attendant who can then approach and rectify the problem.

There are other prominent examples like Gmail that uses machine learning technology to filter emails and provide a safeguard from malicious emails. And not to forget IBM's Watson that extended the power of machine learning for threat detection and cybersecurity purposes.

Anti-fraud technologies on the rise

Of course there are other technologies that have already become popular in reporting frauds. The rise of biometrics is one good example. About one in four organizations (26%) use biometrics as part of their anti-fraud programs; another 16% foresee deploying biometrics by 2021, the study shows.

Also in the next 2-3 years, nearly three-quarters of organizations (72%) are projected to use automated monitoring, exception reporting and anomaly detection. Similarly, about half of organizations anticipate employing predictive analytics/modeling (52%; up from 30%) and data visualization (47%; currently 35%). In all, more than half of organizations (55%) plan to increase their anti-fraud tech budgets over the next two years.

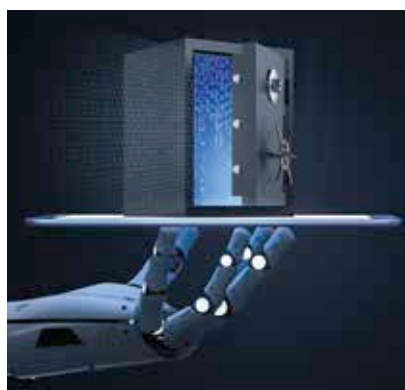
James Ruotolo, Senior Director of Products and Marketing for Fraud and Security Intelligence at SAS believes, “The dramatic rise of AI, machine learning and predictive modeling reveals that, beyond the hype,

advanced analytics is helping investigators keep steps ahead of increasingly sophisticated fraudsters.”

The risks and the rewards

However, the researchers believe while AI can be used to effectively combat cyber threats, it can pose several challenges for the cyber systems and the CIO.

On one hand, by tracking and analyzing data and different patterns, an AI-based system can quickly detect the cyber threats and vulnerabilities and can give timely alerts to CIOs to address these problems promptly. On the other, it often remains vulnerable to malicious cyber programs that can imitate AI-based algorithms. A com-



With the majority of respondents planning to increase spending on AI-ML technologies in 2019, CIOs will need to improve their understanding of these tools to see maximum value... businesses can seriously secure their business with AI

mon problem is AI-powered security program – that otherwise completes its routine tasks – can suddenly be exposed by a more advanced hacking program based on machine learning.

In another survey by Webroot, nearly 75% of IT professionals stated their intentions to incorporate more artificial intelligence (AI) solutions into their cybersecurity initiatives in 2019. Despite these ambitious intentions, the same study revealed that a staggering 58% of these same respondents don't completely understand how the technology works.

The study researcher believes there are huge knowledge gaps around how AI tools work to secure businesses and streamline operations. With the majority of respondents planning to increase spending on AI-ML technologies in 2019, CIOs will need to improve their understanding of these tools to see maximum value.

Once the learning phase starts, businesses can seriously secure their business with AI. “Apart from saving a lot of resources, intelligent cybersecurity solutions are more proactive to respond instantly and prevent threats in real-time,” it said.

The future of AI in combating threats

So, while promises and threats will continue to remain with AI-based security systems, none of them can actually completely outweigh the other, believe AI experts. The technology will continue to make important value additions by minimizing security tasks with high efficiency of fraud detection.

“As criminals find new ways to exploit technology to commit schemes and target victims, CIO/CISOs must likewise adopt more advanced technologies to stop them,” says Bruce Dorris, report author and President and CEO of the ACFE.

He believes that the future of AI in cybersecurity looks to be very promising. How AI can be used effectively to safeguard the data and processes, will decide their relevance in the future. ■



Automation Is Becoming A C-Suite Priority

With automation, CIOs are seeing an increase in customer engagement and new revenue sourcing

As enterprises across industries are increasingly focusing on digital transformation, experts believe that automation of business processes has made considerable headway and is clearly becoming a C-Suite priority. In fact,

a number of reports this week bring out the fact that the impact of automation can be huge. While they observe several barriers to automation including hundreds of job loss, it is evident that the time has come when we can't simply put a stop on this technology innovation.

C-suite sees gain in automation

A new study released this week by Robotic Process Automation (RPA) and AI software company, UiPath in collaboration with The Economist Intelligence Unit, found that over 90% of organizations already use technology to automate business processes.

The survey polled 500 senior executives of mid and large enterprise in eight countries including, Canada, France, Germany, India, Japan, Singapore, the UK and the US. It shows that 80% of respondents report that the C-Suite is driving automation initiatives for their business, with automation responsibility rolling up to the CEO (22%), CTO (29%) and CIO (17%). Over 70% of C-suite respondents report that RPA and AI are a high or essential priority to meet their strategic objectives, mainly because they expect it will make them more competitive.

This demonstrates that automation is helping businesses in every industry seek efficiencies that come from replacing manual tasks with machine-operated ones. The obvious benefits of automation technologies as cited by nine out of 10 CIO/CTOs are increase in customer satisfaction, focused employee attention on less repetitive and mundane tasks, an increase in customer engagement and new revenue sourcing.

While automation maturity is at its highest in the US, with over 60% of organizations making extensive use of automation, there are some interesting findings from India. The country shows the maximum level of enthusiasm about automation among CIOs and other senior executives. 84% believe RPA is a high or essential priority to meet strategic business objectives for Indian businesses as against the global average of 76%. Also 90% C-level executives expect their company's financial results to improve as a result of automation, namely profitability, operating costs and revenue growth.

Sector wise, IT and manufacturing have outpaced other industries in automating business processes. By

contrast, government and public sector institutions have made the least headway among surveyed sectors. Of CIOs who have implemented automation, most have automated highly repetitive back-office functions.

“Automation of functions is most extensive in IT, operations and production, customer service and finance. Typical candidates for automation in IT have been processes such as password management and the logging of service requests, while in operations, maintenance scheduling is frequently automated,” the study says, adding that in two years, those surveyed believe customer service, marketing and R&D functions will be important to automate.

Not without challenges

However, the C-level offices believe that automation comes not without its challenges. Like any new technology, there will be factors holding companies back from complete implementation. For automation, data privacy and security concerns top the list. This has been especially emphasized by CIOs of public companies and healthcare executives.

Executives also site deployment of technology, lack of relevant talent and skills, and employee resistance as barriers for business-wide automation adoption. The skills gap is felt most acutely in Asia, particularly Japan, while change resistance is most prominent in the UK. For those reasons, 42% of executives believe providing education and re-skilling opportunities are very important to smooth implementation.

Nonetheless, the EIU study concludes that automation will accelerate human achievement and that 80% believes that automation is most effective when it complements humans, not replaces them.

A Gartner report released this week also shares similar ethos. The study finds the RPA market grew over 63% last year, enabling customers to bring a level of automation to legacy processes without having to rip and replace the legacy systems.

Fabrizio Biscotti, research vice president at Gartner points out that companies with large amounts of legacy infrastructure like banks, insurance companies, telcos and utilities are key driver for RPA projects. By using this technology, organizations can quickly accelerate their digital transformation initiatives, while unlocking the value associated with past technology investments,” said in a statement.

While experts are optimistic that automation technologies like artificial intelligence, machine learning, and robotics are already changing the enterprise landscape for the better, the old debate of humans versus robots comes up yet again when an

Robots need to do jobs that can be automated, and humans need to do the jobs that require a personal or creative touch. And it is here that CIO/CTO can lead this technology

Oxford Economics report this week demonstrates that the integration of AI and robotics could take millions of jobs in the coming decades – and more so in developing economies.

The report (also released earlier this week) reveals that the rise in automation will lead to a loss of about 20 million manufacturing jobs globally through 2030. It means around 8.5% of the global manufacturing workforce could be replaced by robots. Conversely, it tends to produce more new jobs than it automates them, in turn, it could also lead to income inequality, the report found.

However, automation led by AI and robots are the inevitable future. They will continue to play an even bigger role the enterprise, leaving room for decision makers to have conversations on how they can be prepared when the time comes.

How CIO can lead the way

In order to have a productive future, many experts suggest humans and robots need to work alongside each other. Robots need to do jobs that can be automated, and humans need to do the jobs that require a personal or creative touch. And it is here that CIO/CTO can lead this technology changes.

Place value on people

Recognize the range of skills required in the workforce to optimize the potential of technology and to grow the market. Potentially displaced workers could get re-trained to apply their skills elsewhere. CIOs could potentially help in re-skilling to build on their existing skills and work in a different area.

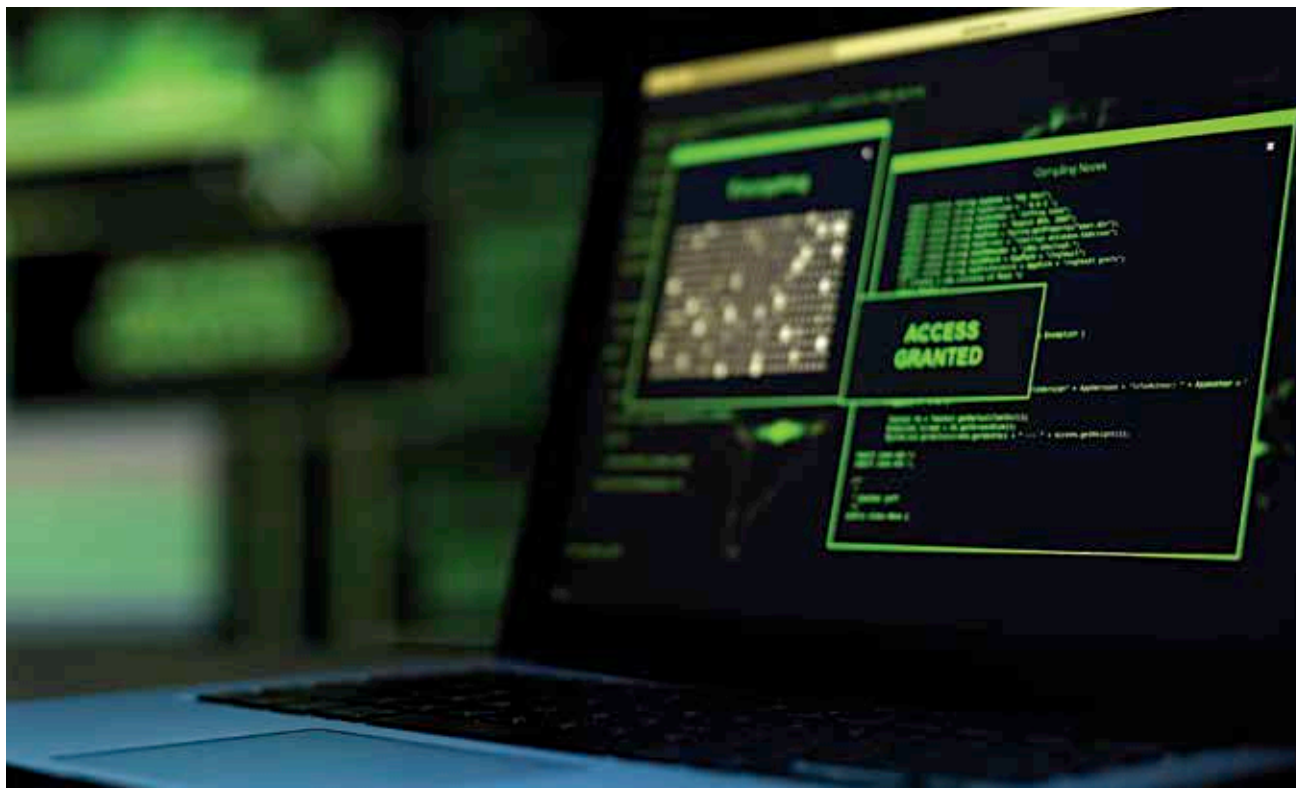
Communicate with C-suite

Constant communication with the C-suite is essential. Do not hesitate to seek technological solutions to your business challenges. The CIO can put steps in place to mitigate the job displacement and societal disruptions robots can create, and help the organization come up with a strategy on RPA, AI and other disruptive technologies.

Innovate continuously to solve business problem

CIOs must think and work in innovative ways to help the organization perform at its very best. It is important for CIOs to create a data driven culture and figure out ways to harness the power of data for the good of the enterprise. For example, disruptive companies like Amazon, Uber and Airbnb thrive on using data to differentiate their products and services—and in many cases, have come up with entirely new revenue models.

Therefore, with C-suite prioritizing automation more than ever, the main takeaway for CIOs is to identify greater revenue opportunities, retrain and coach teams, enhance customer value and drive IT scale and optimization. This would help CIOs lead the way in the world of automation. ■



Rise In Unauthorized Access Incidents A Key Concern For Customers: C-Suite Survey

Consumer confidence is at an all-time low. They want to understand what companies have done to secure their products and services and they are willing to take their business elsewhere if that brand promise is broken

By Nikhil Taneja

Companies are more connected to their customers now than ever before. After spending billions to digitally transform themselves, organizations have exponentially increased the number of touchpoints as well as the frequency

of communication they have with their customer base.

Thanks to digital transformation, organizations are more agile, flexible, efficient, and customer centric. However, with greater access to customers comes an equal measure of increased vulnerability.

One sees the havoc that a data breach can wreak upon a brand; hackers are the modern-day David to the Goliaths of the Fortune 1000 world. As a result, a fundamental shift in management philosophy around the role that information security plays across organizations is taking place.

The savviest leaders have shifted from a defensive to offensive position and are turning information security into a competitive market advantage.

A survey of C-Suite executives to measure leadership sentiment around information security, its costs and business impacts was conducted. Around 263 senior leaders at organizations primarily with revenue in excess of 1 billion USD/EUR/GBP from around the world were approached. Respondents represented 30% financial services, 21% retail/hospitality, 21% telecom/service provider, 7% manufacturing/distribution, 7% computer products/services, 6% business services/consulting, and 9% other.

The report highlights:

- Increased sophistication of management philosophy for information security and security strategy.
- While responsibility for cybersecurity continues to be spearheaded by the CIO and CISO, it is also being shared throughout the entire C-Suite.
- 72% of executives responding claimed that it's a topic discussed in every board meeting.
- 82% of responding CEOs reported high levels of knowledge around information security, as did 72% of non-technical C-Suite titles – an all-time high!
- Security issues now influence brand reputation, brand trust, and consumer trust, which forces organizations to infuse information security into core business functions such as customer experience, marketing and business operations.

All with good reason. The average cost of a cyberattack is now roughly USD 4.6M, and the number of organizations that claim attacks cost them more than USD 10M has doubled from 2018 to 2019.

Customers are quite aware of the onslaught of data breaches that have affected nearly every industry- from banking to online dating throughout the past ten years. Even though many governments have passed many laws

to protect consumers against misuse of their data, such as GDPR, CASL, HIPPA, Personally Identifiable Information (PII), etc., companies still can't keep up with the regulations.

Case in point:

- 74% of European executives report they have experienced a data breach in the past 12 months, compared to 53% in America and 44% in APAC.
- Half (52%) of executives in Europe have experienced a self-reported incident under GDPR in the past year.

Consumer confidence is at an all-time low. These same customers want

Savvy leaders recognize the connection between information security and reputation management

to understand what companies have done to secure their products and services and they are willing to take their business elsewhere if that brand promise is broken. Customers are increasingly taking action following a breach.

Reputation management is a critical component of organizational management. Savvy leaders recognize the connection between information security and reputation management and subsequently adopted information security as a market advantage.

How do companies start to earn back trust?

Leaders today do recognize that security must become part of the brand promise. The research shows:

- 75% of executives claim security is a key part of their product marketing messages.

- 50% of companies surveyed offer dedicated security products and services to their customers.
- Additionally, 41% offer security features as add-ons within their products and services and another 7% are considering building security services into their products.

Balancing Security Concerns with Deployment of Private and Public Clouds

Digital transformation drove a mass migration into public and private cloud environments. Organizations were wooed by the promise of flexibility, streamlined business operations, improved efficiency, lower operational costs, and greater business agility. Rightfully so, as cloud environments have largely fulfilled their promises.

However, along with these incredible benefits comes a far greater risk than most organizations anticipated.

- 54% respondents shared that improving information security was one of their top three reasons for initiating digital transformation processes.
- 73% of executives indicated they have had unauthorized access to their public cloud assets.

What is more alarming is how these unauthorized access incidents occurred

Conclusion

The technical sophistication of the modern business world has eroded the trust between brands and their customers, opening the door for a new conversation around security. Leading organizations have already begun to weave security into the very fabric of their culture – and it's evidenced by going to market with secure marketing messages, sharing responsibility for information security across the entire leadership team, creating privacy-centric business policies and processes, making information security and customer data-privacy part of an organization's core values, etc. ■

The author is Managing Director - India, SAARC & Middle East, Radware



Cyber Security Lapses Can Jeopardize M&A Deals

A new study suggests that CIOs and business decision makers should pay greater attention to cyber risks when considering an M&A deal

Cybersecurity issues are increasingly becoming a concern in merger and acquisition (M&A) deals, shows a new research report. The study conducted by Forescout suggests that IT and business decision makers should pay greater attention to this aspect, when they consider an M&A deal.

The research of more than 2,700 IT and business decision makers surveyed by Forescout Technologies, in seven countries, including India 53% reported that their organization had encountered a critical cybersecurity issue

or incident that put an M&A deal in jeopardy. And 65% of respondents said they had experienced buyers' remorse because of cybersecurity concerns after closing a deal.

A good example can be the Verizon acquisition of Yahoo in 2017, where following Yahoo's security breach disclosures, there was a USD 350 million acquisition price cut.

Cyber risks put M&A deals in jeopardy

There have been a number of challenges and risks involved in various merger and

acquisition (M&A) deals over the years. While financial and cultural risks in an M&A process have always made headlines (and still exists), the most recent spike seen in present day is – Cybersecurity risks – one that decision makers must consider.

As Julie Cullivan, CTO and chief people officer, Forescout believes, “M&A activity can be a game-changing moment in a company’s history, but recent breaches shine the spotlight on cybersecurity issues and make one thing abundantly clear: you don’t just acquire a company, but you also acquire its cybersecurity posture and a potential Trojan horse.”

Here are some key takeaways of the study:

Less time to review, evaluate deals: Proper cybersecurity evaluation takes time, but acquisitions often run on fast track, says the study. For instance, many deals face a race to get across the finish line. Only 36% of respondents strongly agree that their IT team is given adequate time to review a targets’ cybersecurity standards, processes and protocols before completing an acquisition.

Cybersecurity is now a top priority: More focus on cybersecurity risk during M&A is need of the hour. And this is something 80% of business and IT decision makers interviewed have also agreed. Say, 65% respondents said that they are putting more focus on an acquisition target’s cybersecurity posture than in the past, highlighting that cybersecurity is a top priority.

IoT and human error put organizations at risk: When asked what makes organizations most at risk during the IT process, CIOs say, it is both human error and configuration weakness (51%) and connected devices (50%) that cause the jeopardy. According to most CIOs, services often get overlooked during integration (and after integration of a new acquisition) due to the rise unaccounted devices, including IoT and OT devices. Researchers suggest, a company should not automatically trust the hygiene of IT assets. It’s critical to have

full visibility into all connected devices and determine whether they are patched, configured properly and free of malware.”

Prevalence of cybersecurity issues: More than half (53%) of survey respondents report their organization has encountered a critical cybersecurity issue or incident during an M&A deal that put the deal into jeopardy. Further demonstrating the potential consequence of a security incident, undisclosed data breaches have become a



More than half (53%) of survey respondents report their organization has encountered a critical cybersecurity issue or incident during an M&A deal that put the deal into jeopardy... undisclosed data breaches have become a deal breaker for most

deal breaker for most companies. 73% of respondents agreed that a company with an undisclosed data breach is an immediate deal breaker in their company’s M&A strategy.

Internal IT teams may lack the skills to conduct cybersecurity assessments: Among CIOs, only 37% strongly agree that their IT team has the skills necessary to conduct a cybersecurity assessment for an acquisition. Due to lack of resources, organizations must allocate outside resources to their cybersecurity assessments and/or may not be able to complete a robust assessment.

Cyber assessment becomes essential

At a glance, cyber is recognized by CIOs and business decision makers as something they need to pay attention to, because if they don’t, it could stop a deal in its tracks, or result in major financial losses or reputational damages down the road, cautions Cullivan. The CIO, she believes along with the board and other decision makers can play a role in smoothing this process.

In view of this, Cullivan believes that cyber assessments should be a major part of the acquisition evaluation. It is absolutely critical that the assessment of a target company’s cyber posture and the evaluation of potential vulnerabilities start from the very beginning of the M&A process and continue through integration and post-integration.

“It’s important to remember that even if the initial evaluation does not find any significant cyber risks, the target company will continue to operate—with current employees, customers, vendors and the connected world at large—throughout the M&A process. And, at any point, the target company’s assets and devices could become vulnerable,” she cautions, adding that apart from continuous training (on integration and IoT devices etc) and evaluation (on the cyber security strategies), it can be very difficult to develop and maintain a comprehensive view of cyber risks. ■



IT-Based Attacks Increasingly Impacting OT Systems: Study

With OT systems getting connected to IT networks, chances of more attacks increase

As organizations strive to make their operations more agile in response to dynamic marketplace, they try to connect their Operational Technology (OT) systems to the Information Technology (IT) Infrastructure. Now, although there are significant benefits, such as access to real-time market data, major cost savings and effective and efficient monitoring of processes, this connection exposes OT systems to key security challenges. According to Fortinet's *2019 Operational Technology Security Trends Report*, 77% of OT leaders said they experienced a malware intrusion

in the past year and half experienced between three and ten.

The Fortinet *2019 Operational Technology Security Trends Report* analyzes data gathered from millions of Fortinet devices to discern the state of cybersecurity for ICS and SCADA systems. Some of the key trends from the report indicate:

1. Increasing IT-based attacks impacting OT systems

With OT systems getting connected to IT networks, chances of more attacks increase. More and more cyber attackers target IT and OT systems at an organization simultaneously

with the same malware. Since OT systems often use older technology and security operations are frequently less developed, the attackers have a higher rate of success there.

Malware recycling for OT

Cyber attackers are reusing legacy malware packages that were used in the past for IT attacks, but are now caught by any signature-based IT security solution. Figure 1 shows the percentage of existing threats detected by Fortinet during each month of the year, as well as the number of devices with OT protocols hit by any of the threats each month.

The figure shows that the pattern is very cyclical: when more threats are being used, fewer devices are hit, and vice versa. This cycle shows that adversaries are casting about for new vulnerabilities in newly connected OT systems. In the "reconnaissance" phase, they test a wider variety of old malware on a relatively small number of machines. Once they identify the threats that were successful, they move into an "attack" phase, using the subset of attacks that proved successful on a larger number of machines. Their aim is to maximize the value of existing malware before investing in creating new, more targeted attacks.

Another factor may also contribute to this seasonal variation in the use of new versus old threats. Specifically, attacks on heating, ventilation, and air conditioning (HVAC) systems and electrical grids are more likely to occur when these systems are operating at peak usage—most often during the Northern Hemisphere's summer months. The age of an OT system is also a factor, with adversaries tending to target older technology more frequently than newer, more secure technology.

Cyber attackers targeting devices using variety of OT protocols

While IT systems have been standardized for many years on the TCP/IP protocol, OT systems use a wide array of protocols, many of which are specific

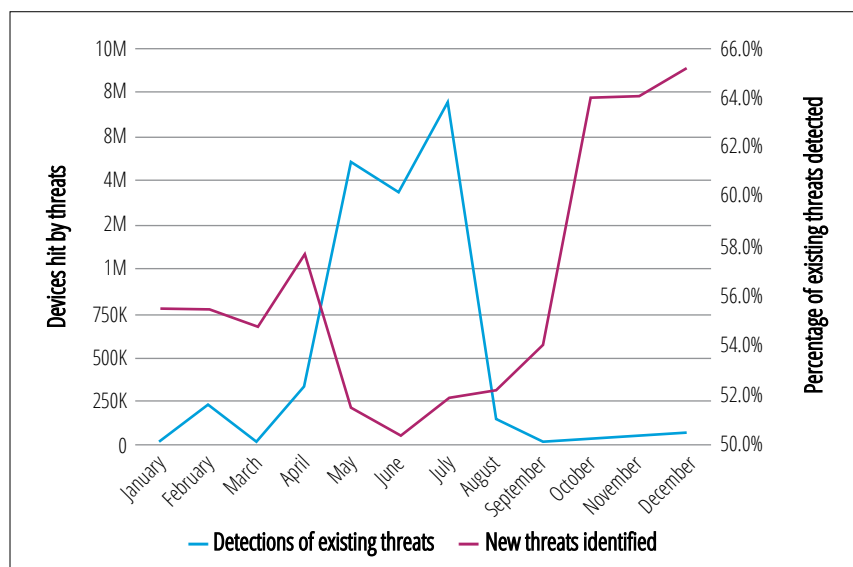


Figure 1: Percentage of existing threats detected and devices hit, 2018

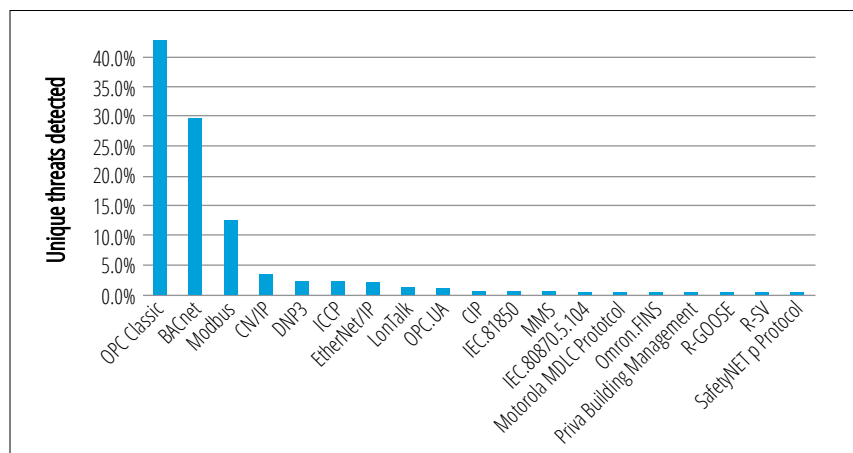


Figure 2: Number of unique threats detected targeting ICS/SCADA protocols

to functions, industries, and geographies. The OPC Foundation was established in the 1990s as an attempt to move the industry toward protocol standardization. OPC's new Unified Architecture (OPC UA) has the potential to unite protocols for all industrial systems, but that consolidation is many years away due to the prevalence of legacy protocols and the slow replacement cycle for OT systems.

Cyber criminals have actively attempted to capitalize on this confusion by targeting the weak links in each protocol. Figure 2 shows the number of unique threats targeting machines using specific ICS/SCADA protocols. Despite seasonal fluctuations and a wide variety of targets,

the data is clear on one thing: IT-based attacks on OT systems are increasing. For example, Figure 1 shows that the spike in new threats detected is much higher at the end of the year than the spike at the beginning of the year.

2. Increasing Malware and Ransomware attacks targeting safety systems

Malware targeted specifically at ICS and SCADA systems has been developed for a decade or longer, but examples are not numerous. OT specific exploits include Stuxnet, Havex, Industroyer, and most recently, Triton/Trisis. Ransomware also continued to attack OT systems. For instance, Not-

Petya Ransomware massively affected both IT and OT systems.

3. OT system attacks transcending geographically

In a global economy dominated in many industries by global players and characterized by extreme connectivity, geography is easy to traverse for legitimate actors as well as criminals. While attacks targeting most vendors were relatively level from region to region, Rockwell and Schneider exploits disproportionately affected North America, while Siemens attacks were more frequent in Asia Pacific. In all three cases, this reflects where the strong markets are for each company. On the other hand, Moxa systems are ubiquitous and heavily targeted around the world, despite the Japan-centric nature of the biggest attack on its users—the Moxa 313 vulnerability.

While the BACnet and Modbus protocols were heavily targeted around the world, EMEA saw the most intense level of detections.

Therefore, a threat landscape should be taken seriously by any organization that has connected ICS/SCADA systems as these have historically been the technology workhorses at many organizations, lasting for decades without major upgrades. The reality of advanced persistent threats requires a more strategic approach—everything from patching to segmentation to access control. It is imperative that those systems are subject to the same level of security protection, the same security hygiene standards, and the same tracking and reporting processes as the IT network. Otherwise, the OT network will be the weak link through which adversaries are able to infiltrate and gain access to critical systems and data—both OT and IT.

To make this happen, the IT and OT functions in every organization need to overcome the cultural challenges brought on by their past isolation. The groups must come to understand each other's values so that a mutually beneficial relationship can be forged for the future. ■



Single Sign-Ons To Accelerate Growth Of Digital Identity: Study

This is one of the key trends impacting digital identity, the others being multiple logins and blockchain

It is important to know 'your identity'. Every organization wants to know, from the e-retailer to the tax office to the bank. However, there are 2 main issues with this:

- It is very easy for fraudsters to exploit the system when all that is required is an email address or password.
- When the burden of proof is higher, this can be highly problematic for users.

These users might have to supply passport numbers, bank account details, and letters from employers and so on. This information is hard to access and time-consuming to enter,

particularly when, given the continuing digital migration, consumers have to re-enter the same information for a multiplicity of services. Furthermore, with that information now being stored by numerous online providers, it increases the risk (and the consumer's perception of the risk) that the data will be exposed and potentially misused. The ability to either create or impersonate identities is a problem for many businesses, particularly those handling financial data.

This is due to multiple points of failure in conventional identification and verification processes, particularly for

online payment details but also in a variety of other sectors. Passwords and centralized repositories have both been highlighted as the core issue within the growing problem of identity fraud.

According to Juniper Research, having a secured digital identity is of paramount importance. With regard to this, there are three key market trends which accelerate the growth of digital identity. They are:

1. Multiple Logins

Digital identity online for many consumers is currently a series of separate identities with distinct credentials and authentication methods, typically passwords in the latter case. This has led to many different 'islands' of data, which are typically stored in centralized data silos held by each online entity that requires such information. This has created a variety of inefficiencies, which companies have typically solved through consolidation of passwords into additional repositories in the form of password managers, or password retention tools integrated directly into browsers or other programs requiring authentication.

Credential reuse is one of the biggest problems with identity management, as it enables credential stuffing; the practice of applying stolen credentials across multiple sites a fraudster to access more data illicitly. Where credentials are not shared, this is not possible. The complexity inherent in having multiple logins has encouraged large companies (most notably Google and Facebook) to federated identity provision for consumers through their platforms. Federated identity provision is also typically part of enterprise SaaS (Software-as-a-Service) provision, where logging into a device can also grant a worker access to cloud provision of services. This is typically done through a format whereby requests are sent to an identity provider and then tokenized, such as SAML (Security Assertion Markup Language), OpenID and OAuth (Open Authorization) protocols.

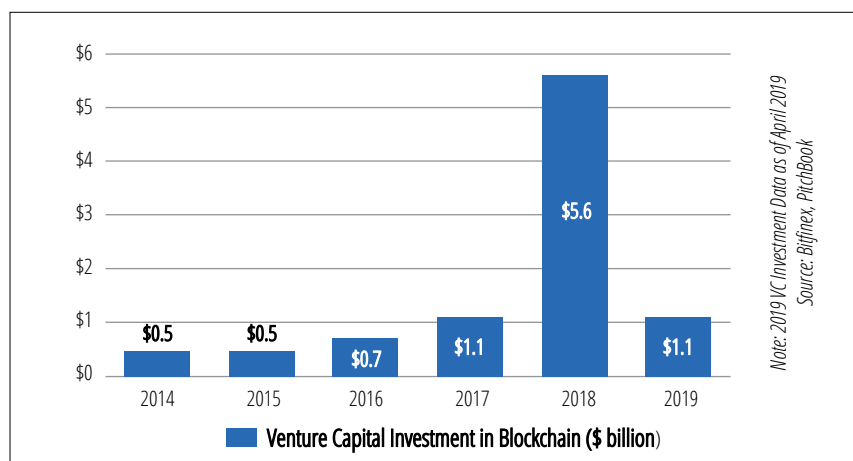


Figure 1: Blockchain Venture Capital Investment, 2014-2019 YTD

2. National single sign-on initiatives

Many countries have recently planned, or are planning, to bring digital identity to many citizens. It will have an effect on the kinds of digital identity security available to consumers, as many of these initiatives are intended to bring identity verification to those who have never had official identification. That being the case, these schemes need to be accessible to those with low levels of digital access, and are likely to be SIM-based, rather than relying on an online presence as such.

These initiatives will also be more likely to have a physical card than other forms of digital identity. This impacts a range of use cases and allows a more consistent application of identity verification than in the case of identities that do not connect to a physical asset. This is frequently because the core documentation on which the foundation of the identity is built contains a photograph as the core verification method.

Other methods (such as fingerprint sensors) require additional infrastructure and do not eliminate the chance of presenting false data at the point of on-boarding.

So such national initiatives need sufficient drive behind them to establish a large enough addressable base.

3. Blockchain hype

Despite cryptocurrencies' fluctuating

fortunes, blockchain as a technology continues to attract increasing levels of investment (see Figure 1). With many still sceptical about the promise of cryptocurrencies as viable alternatives to fiat currency, the underlying technology is being applied in other areas at levels sufficient to keep investment high.

One of those use cases is in the self-sovereign identity movement, which typically uses a blockchain to keep a record of who has validated what credential. The credentials themselves are stored in a digital wallet contained on the user's smartphone, which then sends tokens validated through the blockchain to the requesting entity.

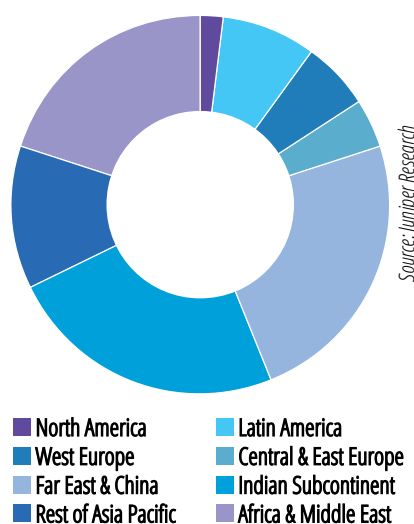


Figure 2: Number of People with a Digital Civic Identity, Split by 8 Key Regions: 5 Billion in 2024

This removes the need for a central database that could be a rich source of credential information.

However, the companies issuing digital identities through blockchain in particular need to grapple with the problem of credential revocation. This can be solved through the blockchain updating a revocation registry and the identity verifier then checking the revocation set to see if a credential is still valid. However, the perception of blockchain as an indelible record is likely to create the image of irrevocable credentials, which will hold the technology back from its full potential.

Civic digital identity forecast

According to Juniper Research, over 5 billion people worldwide will have a civic digital identity document by 2024, from an estimated 1.7 billion at the end of 2019. This will represent 74% of people who have any form of identity document at all.

The growth of digital identity will be at a CAGR of 26.1% throughout the forecast period, with some of the slowest markets being in areas like West Europe and Australia. The biggest opportunities for this market lie in Africa. Here, countries unencumbered by legacy systems are following Estonia's lead of rapid digital identity development. Governments typically provided such cards, which many people in more developed countries have previously rejected.

As per Juniper Research, markets across Europe and North America will be led by the financial services sector and digital driving licences, rather than formal government identification.

Mobile single sign-ons will be a large part of several digital identity platforms, with over 1 billion users by 2023; generating over USD 5 billion in revenues that year.

Blockchain and the self-sovereign identity movement are part of this future, but will be a small piece of the puzzle. Despite average yearly growth of 35%; less than 10% of dedicated identity apps are expected to be blockchain-based by 2023. ■



Two times
the revelation



Dhruva Vijayvargiya

Senior Manager
JLT Group

MY FAVORITE MUSICIAN

Lata Mangeshkar



MY TECH IDOL

Steve Jobs



MY FAVORITE ACTOR

Sanjeev Kumar



MY PASSION IN LIFE

Gardening & Solar Power Generation

MY PEER IN THE IT
COMMUNITY

Sreejith G, Head -
Datacenter Operations,
Sify Technologies



Sreejith G

Head - Datacenter Operations, Sify Technologies

MY FAVORITE BOOK

Wings of Fire by
Dr. APJ Abdul Kalam



MY FAVORITE CUISINE

Fish fry



AN EMERGING TECH THAT I
WOULD LIKE TO WORK ON

Datacenter Information
Manager (DCIM)

A TECH SHOW I
ATTENDED RECENTLY

Datacenter Dynamics Event on 'Datacenter
Emerging Technologies' held in Mumbai in 2018

MY FAVORITE SPORTSPERSON

Kapil Dev



डिजिट अब हिंदी में

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

di9it.in
NOW IN HINDI



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

डिजिट

DATA CENTERS DESERVE PERFORMANCE. RELIABILITY. CONSISTENCY.



EXPERIENCE

For more than 30 years, Kingston has been an integral component in the IT backbone of Fortune 500 companies. An experienced business solutions partner, Kingston offers products with consistent and reliable performance along with award-winning solutions required by enterprise environments.

SATA 3.0 (6Gb/s)



Server Virtualization



Cloud Computing



IT Applications

MEMORY | SSD | USB DRIVES | FLASH CARDS

For sales enquiry: sales_india@kingston.com
Service toll no.: 1860 233 4515
RMA/WARRANTY: services_india@kingston.com,
For technical support: techsupport_india@kingston.com



Quality of Service (QoS) | Predictable Low Latency | Consistent I/O Delivery

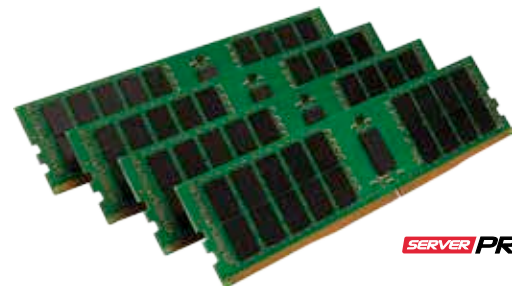
Enterprise Solid-State Drives (SSD)

Incredible Speeds With Full Security Suite.



Server Memory

Accelerate Performance



SERVER PREMIER



©2019 Kingston Technology Far East Co. Ltd (Asia Headquarters) No. 1-5, Li-Hsin Rd. 1, Science Park, Hsin Chu, Taiwan, R.O.C.
All rights reserved. All trademarks and registered trademarks are the property of their respective owners. MKF - 862.1