Case Study | Pg 14
A Case For Simplicity

Insight | Pg 22
PKI's Role In Forging Digital Trust

ITNEXT
FOR THE NEXT GENERATION OF CIOs

2010–2019 LOOKING BACK

Eight defining trends that marked the last decade; their genesis and impact

November 2019 | ₹100 | Volume 10 | Issue 06 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

PAHWA™ GROUP
Innovation is life

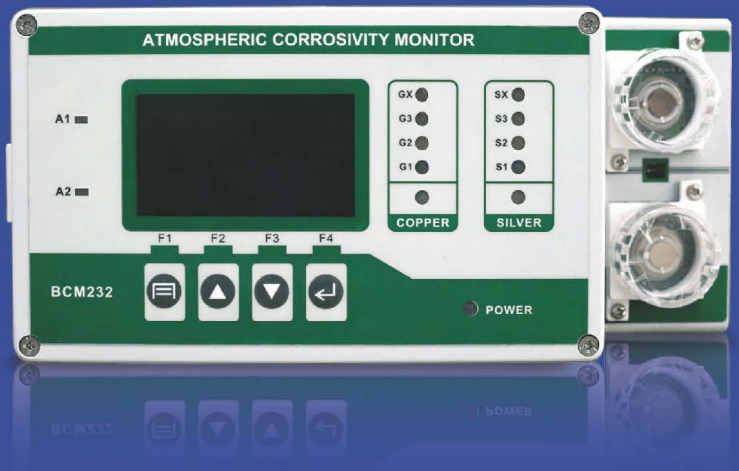
CORROSIVE GASES ARE NO LONGER INVISIBLE

Bry-Air

Read their corrosion potential on

Bry-Air®

Atmospheric Corrosivity Monitor (ACM)



Enables you take timely action
before equipment breakdown in data centers, server rooms, DCS rooms, switchgear rooms

Contact today!

Backed by Brycare™ Service

BRY-AIR (ASIA) PVT. LTD.
www.bryair.com
Phone: +91-124-4184444 • E-mail: bryairmarketing@pahwa.com
Plants: India • Malaysia • China • Switzerland • Brazil • Nigeria
Overseas Offices: Vietnam • Indonesia • Philippines • Korea • Japan • UAE • Saudi Arabia • Bangladesh • USA • Canada

RB/BA/1922FCA3

Leaders in Gas Phase Filtration Systems

2010-2019: Five things that changed for you

With the IT delivery part increasingly going outside the boundary of organization—to outsourcing providers and cloud service providers—the center of gravity for IT manager is shifting more towards the demand side—of helping businesses with strategic use of IT

Shyamanuja Das

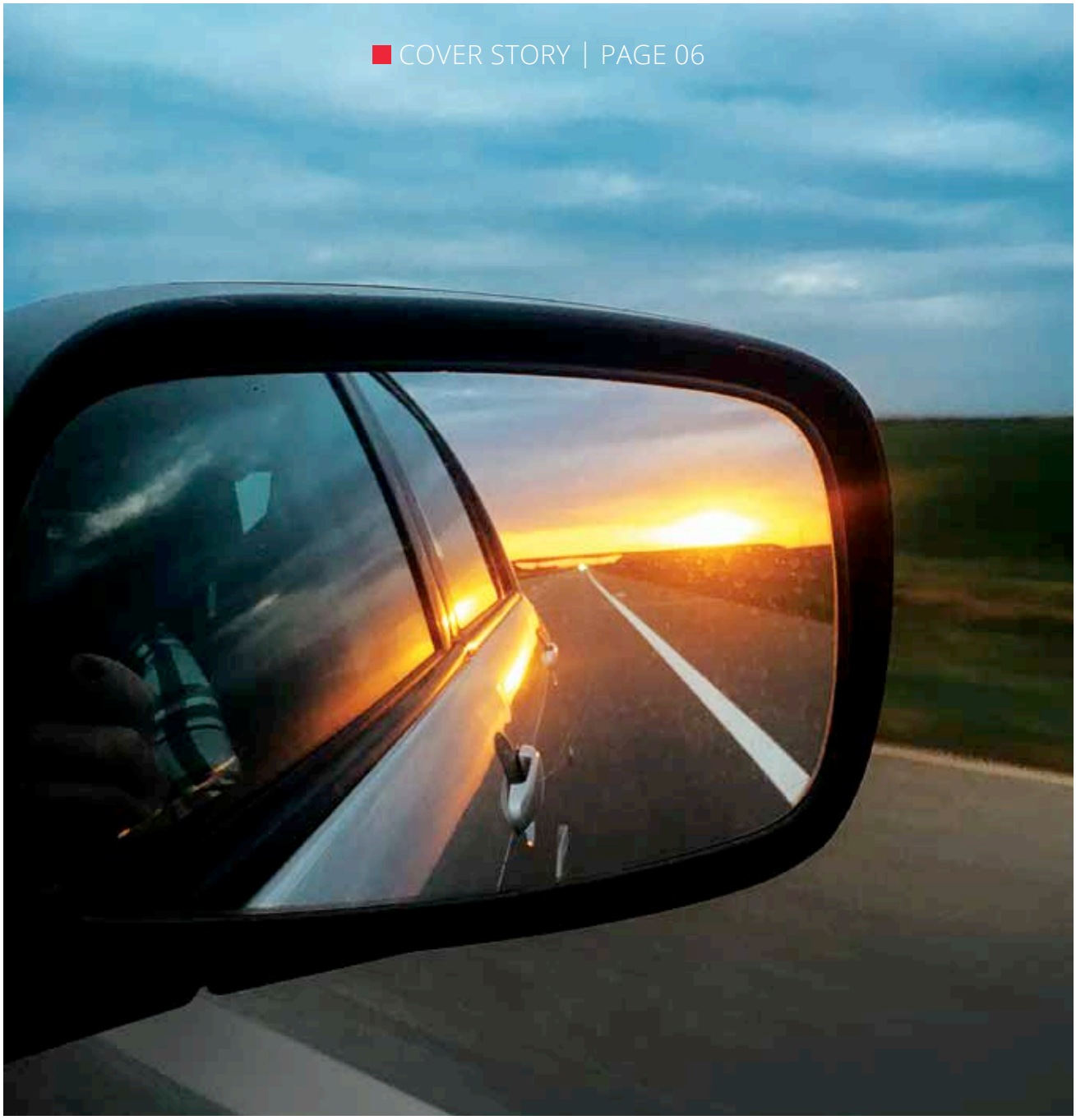
Our cover story this month is on the last decade—major trends that impacted enterprise IT. But let us take a couple of steps backward and look at what changed for IT managers—the people who contributed to these trends.

Let me put here five ways in which your roles—and correspondingly expectations from you—changed:

1. **From controllers to value creators:** This is the most obvious one and strictly, the process began earlier than 2010. As IT ceased to be seen as cost centers and more are business value creators, the expectations from IT managers changed from controlling IT spends and budgets to helping create new opportunities for the business. Correspondingly, the size of the budget you handle is no more the measure of how important your position is.
2. **From suppliers to strategic consultants:** Every IT manager wears two hats. The first is to help business decide how they can use technology to meet their desired business metrics and do more. The second role is to build and manage those technology services for the business. With that part increasingly going outside the boundary of organization—to outsourcing providers and cloud service providers—the center of gravity is shifting more towards the demand side—of helping businesses with strategic use of IT.
3. **From implementors to integrators:** With consumerization of technology—that is users having a say in what technology to use—thanks to better UX, SaaS model and more awareness about IT, there is considerable amount of technology purchase and implementation that is happening outside IT department. Yet, for businesses to realize true value from those investments, these siloed applications must talk to each other and share data. So, integration is becoming more important than implementation, as cloud more or less removes the need for later. It is only the IT department that can do that effective integration.
4. **From problem solvers to proactive innovators:** In the earlier model, IT always followed business decision. So, IT managers expected a very clear and precise definition of problem to be able to find a solution. With organizations using emerging technologies proactively, the question has changed to how one can use a particular technology in the specific business contest. IT managers need to work with business managers to find those opportunities.
5. **From inside-out to outside-in thinkers:** In the above-mentioned change, what becomes necessary for an IT manager is not to get deeper into a particular technology but to exactly know what the emerging tech landscape is like and choose what technology can help their business and how. So, instead of first having a problem and then going out to look for technology (inside-out), he/she should get the landscape first and bring it into the enterprise (outside-in). ■

NOVEMBER 2019
VOLUME 10 | ISSUE 06

Content



Cover Design:
ANIL VK

ADVERTISER INDEX

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
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

9.9 GROUP

EXTRA Curricular

Travelling is an eyeopener; it adds to your personal and professional life

Igniting The Wanderlust Within

NEXT100 Winner 2011 **Ram Yadav,** Founder, DigiVito Solutions LLP, shares his intense passion for traveling and exploring new places...

"Stop worrying about the potholes in the road and enjoy your journey"
- Babs Hoffman

"I travel not to go anywhere but to go. I travel for travel's sake"
- Robert Loius Stevenson

I love traveling and am associated closely to nature. Adventure is in my blood. During college days, I went on a 800+ km adventure cycling expedition from Faridabad to Mussourie. I wish to continue with the spirit of adventure and exploration of the world.

After superannuation from Hero MotoCorp, I traveled to the US with my family. There I visited the Niagara Falls, which happens to be the largest natural horseshoe falls in the world.

Prior to the US, I travelled to Japan, Indonesia and Thailand. I enjoyed the rides in Disneyland as much as I loved the beauty and culture of those places.

I have been traveling within the country extensively, exploring and appreciating the diversity and richness of India's culture and beauty – with the huge rocks in Mahabaleshwar, to the beautiful palaces of Jaipur, cool lakes of Udaipur, Nainital and the quaintness of Mount Abu. I have lans to travel to various destinations in Europe, Australia, and New Zealand by the end of 2020.

During my travels, I not only visit the historic monuments, but also make it a point to visit various industries. My expertise in Supply Chain and Business Process Simplification and Automation, gained over three and a half decades of working for Hero MotoCorp (formerly Hero Honda), allows me to see and absorb the varied practices, trends and different ideas prevalent in other countries.

The skills and experience you gain from traveling can give you lifelong personal benefits in the professional world. It also helps you attain mental peace and satisfaction which later provides a boost to the individual to perform better. ■

As told to Dipanjan Mitra, Team ITNEXT

Ram Yadav

Snapshot

Ram Yadav is Founder of DigiVito Solutions LLP. He is NEXT100 Winner 2011. Earlier, he was associated with Hero MotoCorp for over three and half decades in various leadership and managerial roles. Ram has completed his PhD in Project Management from Indian School of Business Management & Administration.

The doctor at home who cures most ills with his eclectic combination of traditional medicinal plants and yoga

Fusion Of Plants, Ayurveda And Naturopathy And Their Interplay With Tech Life

NEXT100 Winner 2017 **Dhruva Vijayvargiya,** Senior Manager, MMC Group shares his passion for plants, ayurveda, naturopahy and how these help in his tech life...

My love for plants has been there since long. The space constraints of Mumbai made me look for avenues to have plants in a small space. It made me try out balcony gardening and hydroponics. I have grown wheatgrass and chickpeas plants using this technology and am currently working on creating a vertical garden in my balcony. Even when in the US, I had plants which I took care of and was able to grow despite cold, snow and limited sunshine.

The love for plants makes me look at solutions to some of the problems around us through plants. So, for fighting pollution (inside the house), I have plants like Spider plant, Aloe Vera and Fern. For healthy food (because of Ayurveda), I have plants like Tulsi, Lemongrass, Ajwain leaves, Brahmi, Adulsa and plants that help in diabetes and have a positive effect on the physical and mental well-being besides assuring fresh and good quality food on the plate.

My family has also joined me in my efforts but their motivation is to make the house and surrounding look beautiful. Therefore, we have plants like Peace Lilly, Enturiam, Lilly, Bhrama Kamal and many other beautiful looking plants.

For taking care of plants, I use organic manure and organic pesticide. I have a wormiculture basket where I produce the manure for my home garden. For pesticide and vermicides, I use home-made preparations and only as a next step, go for organic pesticides from the market. I do this because I use these plants in my naturopathy preparations and do not want chemicals to be inadvertently injected by me or my family.

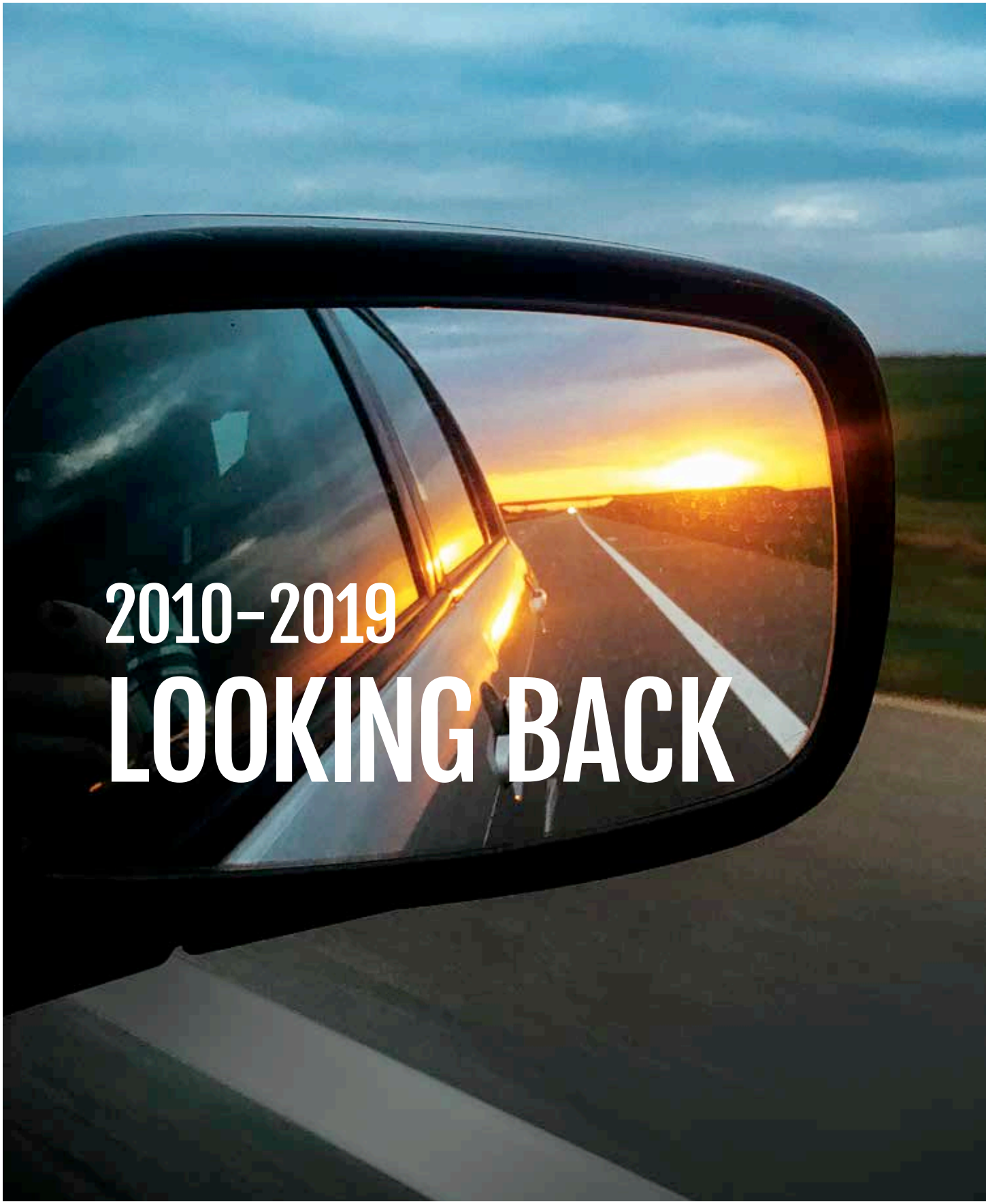
The challenges of today's continuously-on-the-run, hectic life with pressures has led me to develop my other related hobby further, that is Ayurveda, Naturopathy & Mudras. Any disease has 5 different levels of manifestation before it becomes life threatening and if intervened in early stages (level 1 or Level2), the disease and pain is unable to manifest. I use different combinations of ayurveda and yoga to get solutions. This is where my love for plants, naturopathy and ayurveda merges. Taking care of plants reminds me of the technology life which is my work life. There we find newer solutions for the new set of challenges as and when they emerge so as to maintain and create new business proposition. Learning and experiment from one field are truly having a positive impact on the other part of my life. ■

As told to Dipanjan Mitra, Team ITNEXT

Dhruva Vijayvargiya

Snapshot

Dhruva Vijayvargiya is Senior Manager at MMC Group. He is NEXT100 Winner 2017. Earlier, he was associated with companies like Infosys, Oracle Consulting and ICICI Lombard. He has done his PG Diploma in Enterprise Management from IIM-Bangalore and Bachelors in Engineering from Govt. College of Engineering, Pune.



2010–2019
LOOKING BACK

DEFINING TRENDS THAT MARKED THE LAST DECADE; THEIR GENESIS AND IMPACT

By Shyamanuja Das

We—that could refer to as broad as the global economy to as narrow as the Indian enterprise IT community—entered 2010 with a lot of doubt, apprehension and even fear. The second half of 2008 and almost the entire 2009 were filled with disbelief, panic, despair, readjustment and finally caution, in sequence. Sure, the subprime crisis in the US had started well before in 2007 but till October-November 2008, its impact on India was still being debated. And then, it came suddenly. Vendors of consumer technology were still planning big for the Diwali sales, and then it hit suddenly. The wide variance between shipping data and the purchase data—the two data points analysts (this writer included)—track has probably never been seen before—and after.

So, the mood was subdued; the expectations were modest, if not minimal. If measured by that account alone, the decade of 2010-2019 has been impressive. Sure, Indian IT—often identified globally by its exporting IT services firms—adjusted to single digit/lower double digit growths, as compared to 20% plus growths in the previous decade, marked by the spectacular rise of offshoring (read India) of both IT and business services, accepting it as the new normal but the story of Indian domestic technology market—and what we discuss here is a component of that, the B2B tech market, has surely been significant and defining.

A clarification before you jump to conclusions about the scope of the story. While it does begin by talking about market growth, recession and the numbers, it is not about the market per se. It is about trends in enterprise IT—technology, deployment, management, leadership, and the external trends that impacted it.

Recalling the mood prevailing at the start of decade was meant to provide a perspective on where we started from and where we have traveled to.

As a publication focused on the senior enterprise IT managers community, we have seen some of these changes from too close to be able to take a very dispassionate—and as some say, objective—view. Rather, we can just claim it to be an informed, and more accurately, an involved, view. Comprehensiveness is not even attempted.

We tell the story through eight distinct but not always mutually exclusive trends.

Consumers influenced enterprise IT heavily—and in multiple ways

The decade began with a lot of talk on consumerization of enterprise technology. What it meant at that time was a very definite—and in hindsight, we can say very limited—trend of more demanding users within enterprises. It was taken from the word 'consumerism' in the marketplace.

In 2019, when we look back, we can easily say that consumers and consumer markets influenced technology decisions, deployments and management in enterprises in many ways.

First and most visible is the rise of mobile data and how it has impacted businesses, B2C businesses most definitely but even B2B businesses. Today, almost every part of the customer value chain—marketing research, branding and promotion, selling, customer service, support—has seen mobile app intervention. Today, it is no more an innovation; it is the new normal.

The second is application of new technologies to customer-facing functions. Chatbots today are the most visible applications of Artificial Intelligence. And all that has happened in this decade—the second half of the decade to be more precise.

The B2C platform businesses—where aggregators came from nowhere to disrupt 100-plus year-old stable industries—have become the poster boy of technology-led disruption. Every business—B2B businesses included—want to be like an Uber or an Airbnb.

Talking of India, one specific area that has seen revolutionary change is payment. What years of thrust by the previous government and some high-profile plans of this government could not achieve—diffusion of technology-leveraged financial services—has been achieved today by the concerted effort of government policymakers in relevant areas. Demonetization, pragmatic regulatory changes by RBI and efforts by pioneers such as Payment have made common people use electronic modes of payment. That has resulted in all B2C businesses optimizing their processes to the new paradigm.

And finally, within enterprises, the 'consumerization' of technology has moved from mere demanding users to organizations aping popular consumer app marketplaces like Apple Store and Google Play to make apps available to users on not just of their likings but much the same way as they get them on these platforms.

Indian consumer has always been less demanding. Unlike in mature markets, in India, the rise of consumer voice happened largely in these ten years and was driven by technology to a great extent. That is by far the single most big impact that technology has had on Indian business in this decade.

Decade of the Cloud

As a concept, cloud as 'Cloud' made its entry into the enterprise space in the previous decade, especially after Amazon launched Amazon Web Services. But it is in the decade of 2010-2019 that cloud got wider recognition and by 2015, it was clear that the move towards cloud model is irreversible.

If one looks at Gartner Hype Cycle, cloud computing made its first appearance in 2008 and had moved to the Peak of Inflated Expectations by the next year. At that time, the biggest concern was security and the biggest advantage that was being talked about was being able to turn Capex to Opex. This is probably the only technology that CFOs pushed their CIOs to go for.

Like many new technologies, it took some time before people realized the real business advantages of cloud. To startups, it was a great equalizer. To CFOs in large enterprises, it was a great capex saver. To CIOs, it was a way to concentrate on what they were, for long, expected to do—think of providing business value to IT beyond automation-induced efficiency.

Cloud effectively sealed the way for large scale outsourcing, which was beginning to make its presence felt in India, induced by the halo of the global outsourcing wave in the previous decade, led from the front by Indian services firms. Cloud erased the last existing line in IT—between products and services. Microsoft, Oracle, Google turned services companies even as Amazon, a retailer made arguably the largest impact in B2B IT in the last 30 years.

After the hype, by the mid-2010s, pragmatism prevailed, as IT managers realized that moving everything lock, stock and barrel to a cloud of Amazon or IBM or Microsoft, was not the IT salvation. At least, it was not that easy. Hybrid cloud/hybrid IT made its debut. Private cloud made its appearance in Gartner Hype Cycle in 2012 while Hybrid cloud appeared two years later. It continues to rule the roost at the turn of the decade—that is today.

Cloud has moved from being a technology model to a business model enabler to an innovation catalyst to a philosophy. Nothing has impacted enterprise IT the way cloud did in these years 2010 to 2019. It is surely the technology—oh, wait, it is a model—of the decade.

Digital Transformation was (and still is) the business zeitgeist

Interestingly, much of the decade was spent by pundits differentiating between IT and digital. Except that IT is a noun and digital is an adjective, we are yet to understand where exactly one ends and the other begins—or should one say just the reverse?

Digital was not a new word. It existed as an antonym of analog, owing its origin to binary digits but interpreted by the general public as something that shows a quantity—time, speed, volume, weight, temperature—in digits, as opposed to through movement of a needle.

Digital probably entered corporates through the consumer marketers' route (as in digital marketing) and stayed, for some time, as an adjective of any major tech induced change on the consumer side but slowly spread in meaning to become the go-to word for any major change that involved any big or sharp change, as opposed to incremental change; that is when it made its now-famous association with transformation.

As expected, it was overused and abused by vendors, with more than a helping hand from obliging members from journalists and analysts.

But towards the later part of the decade, big transformational change did happen leveraging IT, which was very different in its basic nature from what was seen hitherto. For one, data slowly but steadily did become a decision driver, in all companies. Technology started moving beyond operational processes and began impacting products and business strategy (business models). Certain technological developments (discussed separately) brought manufacturing companies, so far, a little behind, to the forefront of technology-leveraged change. Established rules and equations of year-old industries got demolished by newcomers. Transformation was happening at all levels. Many companies started appointing digital officers or transformation officers.

If cloud was the most common on-the-ground change that IT organizations were initiating, digital transformation (often 'leveraging' cloud) became the most aspirational change for them. It remains a journey, even as we enter a new decade.

Did IT become a little too important to be left to the IT managers?

If two of the already mentioned trends—consumerization of technology (more demanding users) and an overt fascination for big changes induced by technology/digital—resulted in non-tech users dreaming of carrying out technology-induced change themselves, what gave them ammunition to realize those dreams are the emergence of cloud, especially Software-as-a-Service (SaaS) model and the increasing shift towards user experience resulting in products that are far less intimidating for non-techies.

With many functions—such as marketing over the web and mobile and analysis of data, done by many different functional executives—becoming tightly interwoven with technology, it was becoming increasingly difficult to break them into tech and non-tech pieces and get the centralized IT department to do the IT part, for each process and sub-process. That is when SaaS made its debut. Not only did it remove the need to involve the IT team in every functional tech-leveraged work, it also removed a major organizational barrier by removing the need for new IT infrastructure and thus eliminating the need for capex approvals. As software became a service, the expenditure became another opex spend, well within the authority of the functional manager to approve those spends. This kicked off the rise of breaking away from the centralized IT. Smart vendors introduced freemium models (as in consumer services) which allowed these managers to get them familiar with the new applications and buy when they were absolutely hooked to it. Many companies used this strategy along with great UX to hook functional managers. This shift began in the latter half of last decade.

If anything, in the beginning of this decade, concerns started as there were challenges of integration later with enterprise IT systems and that is when corporate IT was needed. But by then, in the organizational power equation, the center of gravity had shifted substantially. Both the groups met halfway and what was considered exception—even rogue in some organizations—got legitimacy.

What made the debate alive again is the announcement by Gartner in 2012 that CMOs would spend more than CIOs on technology (later corrected to business technology).

While marketing was leading the rebellion, other functions too were seeing specialized vendors pitching to functional managers directly.

It culminated in the appointment of chief digital officers by organizations. though there was a tug of war between IT and marketing to be the legitimate claimant to the position, most organizations (especially in India) appointed neither IT nor marketing executives to the position but appointed senior core business executives to that position, whose brief was to drive organizational transformation. Many later called them simply transformation officers. Of late, we see IT managers getting appointed to that post in some organizations, with blessings from CFO who trusts them far more than he trusts marketing managers.

This probably remained the single most fear/worrying factor for the IT managers through the decade.

Manufacturing caught up with Industry 4.0

Before this decade, information technology had been applied in 'services'—that is the services businesses as well as the services components of manufacturing such as HR, finance, supply chain and warehouse management. Something called plant automation existed which used technology—often proprietary—to enhance efficiency of the production process, in what was essentially a closed loop system.

The advent of the likes of Internet of Things changed that dramatically, by connecting the manufacturing system to the enterprise IT, resulting in not just efficiency gains, but timely operational decisions and more importantly, informed decisions by the company management on manu-

facturing. This led to manufacturing companies leapfrogging to make strategic use of technology, the way services companies had done so far.

So important was the phenomenon that the top global think tank, World Economic Forum, coined a word for it—the Fourth Industrial Revolution, often written as Industry 4.0. Klaus Schwab, the founder and executive chairman of the WEF, defined it as "a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres." The biological part—the increasing application of these technologies in health as well as AI as an alternative to human thinking—is still not as interwoven, but the bridge between physical and digital has decisively been established. In fact, WEF even made it the theme of its 2016 annual general meeting at Davos, attended by heads of states, heads of businesses and top thinkers, so important was the change.

Technologies like IoT, combined with data analytics technologies, have not just impacted manufacturing companies, but have added value to other businesses as well but they have truly transformed manufacturing's core value creation process.

There is a flip side to all great stories. Manufacturing systems—and similar physical systems like mining, refineries, transportation and other infrastructure systems—getting connected to enterprise IT and the world at large also means they are now no more isolated from the security vulnerability that IT systems have battled for decades. That is the new challenge.

While that is a continuous one-upmanship game with the evil, the value that accrued to manufacturing industries through technology in this decade is unprecedented and it is one of the megatrends that the decade will be remembered for.

Artificial Intelligence was the buzzword

Artificial Intelligence (AI) is one of the oldest concepts in IT that attained popularity in terms of real application only now. The term itself was coined in the 1950s by John McCarthy. AI, in its comeback years in the 80s, aimed to replicate human intelligence in machines.

The new AI, as we see it today, started in the late 90s, to leverage huge computing power and the volume of data available. It essentially was about machines learning from data, which essentially is collection of real experiences. Not surprisingly, machine learning is often hyphenated with artificial intelligence today.

General purpose machine intelligence appeared in Gartner Hype Cycle in 2016, while virtual assistants, by far the most popular application of AI, made the appearance a year later, along with smart robots. In 2018, Artificial General Intelligence made the appearance while this year, Explainable AI and Adaptive Machine Learning were featured in the Innovation Trigger phase. If anything, it shows how dynamic the nature of and expectations from AI have been.

In India, enterprises went for low-hanging fruits. The virtual assistants, often called chatbots, in support and customer service lingo, have now become a common feature of most large consumer companies with complex conversations, such as banks, insurance companies and telcos. Another area where AI has got into horizontal applications across industries is IT itself—in security as well as in IT infrastructure management. Besides this, there have been some vertical-specific applications of AI.

But what gets AI to this list is the fact that today it is the most common aspirational tech intervention, which top management demands. And this is one area where there is scope for incremental investment and incremental accrual of business value.

It is likely to remain a hot technology for the next decade—probably moving from buzzword to a common tech intervention much like cloud. Ethics, a much-discussed aspect of AI, is likely to make it to the agenda, especially as the country has announced a national AI policy.

CIOs became business savvy, but still remain problem solvers

As technology became core to business—products, processes and strategy—it became an imperative for a CIO to understand the business and talk the lingo. As the supply side involvement of CIO became less and less after outsourcing and cloud model set in, the demand side—creating value creation opportunities for business leveraging technology—expectation increased.

While in the initial years of the decade, the concept was limited to discussions on CIO platforms, the latter half of the decade saw many CIOs taking the business role far more effectively.

Today, many CIOs do understand the nuances of their respective businesses and the typical needs of their operational processes far better to do IT more effectively. But with the ability of digital technologies to positively transform business being constantly preached to the top management, there is a new desire to proactively use emerging technologies for creating business value. They call it use case.

No surprise, the CIOs are expected to not just understand the business but are supposed to find opportunities for applications of those technologies—the use cases—and help in creating that value. Understanding business thoroughly is just the minimum requirement. They also need two additional attributes—the ability to work on blank canvas and being constantly updated on the emerging technology landscape. This is often called outside-in thinking as opposed to the problem-solving orientation which is an inside-out approach. The expectation is: Someone else exactly defines the problem for them. They are excellent problem solvers.

This, precisely, led to many companies appointing business guys as head of digital transformation.

This ability to think proactively—understanding the business, identifying opportunities to intervene with right tech—is going to be the most important attribute of the successful CIO in the next decade.

Security made it to the top of corporate agenda

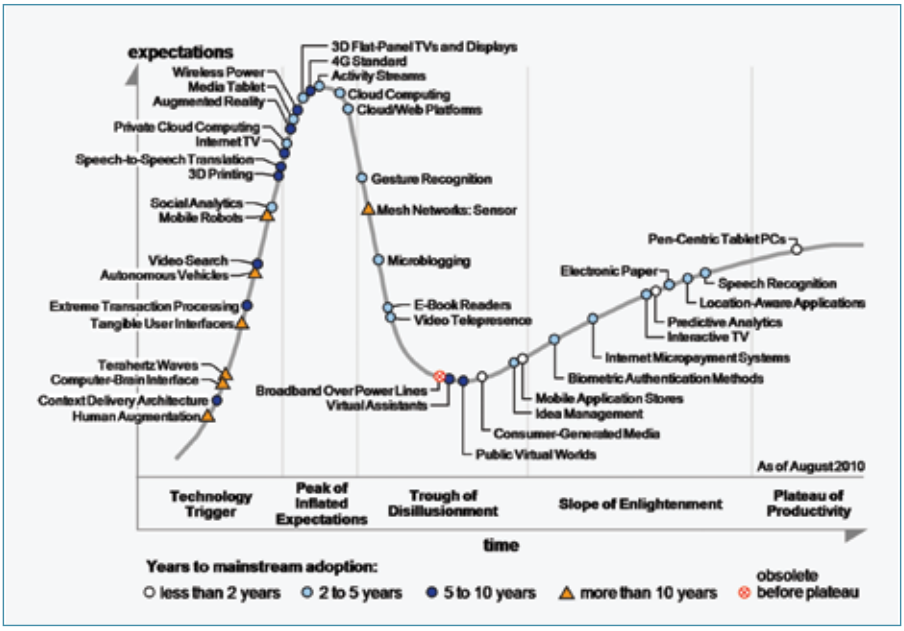
While many buzzwords came and went through the decade, two tech areas saw some real action happening: Cloud and Security. Cloud was a decision; Security was an imperative.

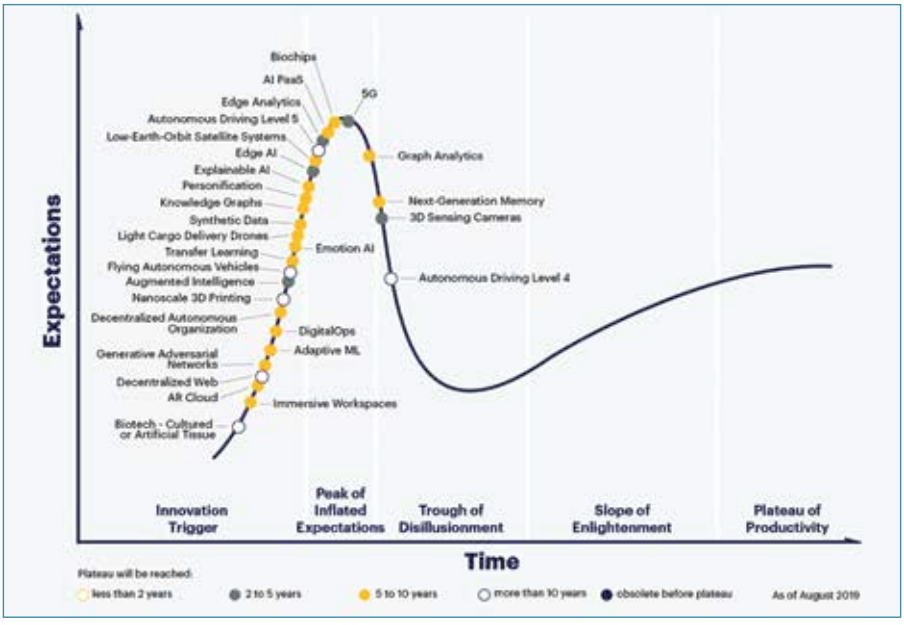
Attacks got more sophisticated and targeted. Data breaches became a regular feature as millions of customers' records were compromised. Some 18 of the top 20 data breaches of this millennium happened in this decade. That was the growth.

While the depth grew, so did the breadth. As people's lives—from education to health, from commerce to entertainment—got more and more vulnerable, the potential vulnerability increased exponentially. And unlike intra-organization policies, businesses had to tread balancing security, privacy and customer convenience—thus making it a tricky game. Emergence of nation states as threat actors also impacted the enterprises.

But one of the biggest threats came from the digitization of manufacturing (refer Industry 4.0 above) which not only made the infrastructure and plants, untouched so far by threats potentially vulnerable, the usage of outdated information technology by many manufacturing OEMs made them especially exposed.

So serious are the risks from cyber threats that from last five years, two security risks—cyberattacks and data thefts—have been featuring among the top ten most likely global risks, ahead of all geopolitical, economical and societal risks and along with environmental risks.





It is not surprising that cyber security has become a top management agenda item. The increasing profile of cyber risks and the need for newer regulatory compliance have made the job of those in charge of security—the chief information security officers—more important. Many of them, who earlier reported to the IT head, have started reporting to Head of Risk. In some regulated industries like banking and insurance, it is a mandate by regulators. Security may not make fancy headlines but will become even more important, as privacy legislation sets in, in India.

The Misses & The Next-in-line

Why these 8? If you have glanced through it, without reading, you would have created a list, would have wondered why so many technologies are missing.

Hopefully, that question would have been answered after reading through the entire piece. To summarize: we were not looking for technologies or buzzwords, we were looking for trends that significantly impacted the way enterprise IT thinks and works in organizations.

That is why a big buzzword like Blockchain is nowhere. True, it was discussed a lot. It held a lot of promise. And we still believe it has potential to bring about revolutionary changes, in some areas. Yes, a few pioneering pilots were done, both by government/regulators as well as by private enterprises. But did it impact larger enterprise IT as a whole? Let alone impacting, it did not even touch.

You can think of many other such examples.

That brings us to what could we expect in the next decade. Difficult for sure (who knew that WEF would make one of these trends its theme for its annual meeting?) but let us try. One that is comparatively easier is privacy. India has already heard the footsteps; a legislation is in the making. Despite Indians not being bothered about individual privacy too much, we expect a big impact of personal data protection laws in everything, including security, business models, campaigns and so on. A long shot is ethics. India is not particularly known for ethics in practice, despite rich literature that preaches and showcases its value. But with technologies getting into our personal lives, there is no way organizations can overlook this aspect. A trend in tech usually starts with the technology companies—there are not too many new tech creators in India—and then percolates down to users. The eagerness to do something about ethics is already visible in the tech circle, with groups focusing on AI, IoT, usage of data, automated vehicles and many other areas. It is a matter of time that we see that in India.

Goodbye to this momentous decade and all the best to all of you for the next! ■

A Case For Simplicity

Startups and small companies value ease of use over everything else while choosing their cloud service provider

By ITNEXT

Marax.ai is a three-year old startup that helps its customers—online service providers and app-providers—to retain their customers and make the latter use their services continuously. It does so by creating personalized offers for the app-users, using Artificial Intelligence (AI).

Marax's integrated Software-as-a-Service (SaaS) solution, MARS, short for Marax Action Recommendation System, uses AI to optimize marketing spend of the app providers.

That sounds deceptively simple.

In reality, what it means every user's journey has to be analyzed and based on the learning, proper action has to be recommended. It can involve a three-stage process:

Identify: Finding out which users are going to leave your platform or become inactive

Diagnose: Finding what has made the user looking at leaving (the reason for possible churn)

Prevent: Prevent the user from leaving by taking appropriate action

The action could involve creating customized offers and sending out personalized marketing messages via relevant channels— push notifications, e-mails, and messages to each customer until the desired outcome is reached.

Marax started with offering identifying potential churn and built up the entire stack in last three years. It was one of the first to do that at individual level.

Since churn in app usage is very high—what with costly mobile phone real estate—it was received very well by the market.

The Challenge

While in a traditional in-premise offering, it is the solution to the core problem, support and pricing decide the

winner, a critical element—availability and reliability—become very critical in a cloud-based offering. That means the cloud backbone for a SaaS-based provider becomes very vital to its basic business model.

It is no different for Marax.

There are four distinct expectations, especially for a start-up working in a cutting-edge technology area.

First, common for any cloud-based services, is availability (and reliability) of the platform.

Second, for a startup working in a new area like AI, there is a strong need for flexibility and functionality, which can support experimentation.

Third, for a small company, the entire proposition has to make sense, not just in pricing but also in terms of support. A small company cannot afford a large in-house cloud team to support the users.

Finally, the platform must be easy to use. A niche startup focuses on its core problem area. The developers and engineers are people with functional expertise in that area and not necessarily cloud experts. It must be easy for them to use.

Marax used two hyperscale service providers who are very good in the first two parameters—reliability and functionality—but they are not necessarily well-suited for startups. But the biggest challenge is ease of use.

That is what prompted Marax to choose DigitalOcean. DigitalOcean—the Developer Cloud for building modern apps—not just offered the best price-to-performance ratio among the cloud providers in the market, it requires very little training.

"The community content and tutorials are just too good," says Prateek Gupta, Co-founder and CEO of Marax.

"For research and experimentation, we allow our engineers to start their virtual machines. It is very easy," says Gupta.

Of course, Marax.ai has one platform for experimentation and development and another for customers. Needless to say, permission levels are different for both.

"The community content and tutorials are just too good"

Prateek Gupta
Co-founder & CEO,Marax

But what about functionality? "Yes, not everything is available, but they are getting there," says Gupta.

The Genesis of the Relationship

Gupta's association with DigitalOcean started when he was still in college. That is when he got a USD 100 referral from his friend to use DigitalOcean.

"I did not even know what a virtual machine means. That was my level of familiarity with the technology," he quips.

But DigitalOcean's tutorials helped him to understand the cloud infrastructure in depth. This is one advantage of DigitalOcean that he swears by. During the conversation, he refers to this aspect multiple times.

When he became VP of Marax.ai, he turned to DigitalOcean and got a credit in December 2018. In January this year, Marax started moving to DigitalOcean. By that time, he had already used two hyperscale cloud providers.

Today, after migrating most of Marax's software to DigitalOcean, he says that the following compelling differentiators make DigitalOcean a trusted cloud partner:

- New memory-optimized droplets ("cloud servers") offer more RAM per CPU. As Marax's approach to processing data needs more RAM power, DigitalOcean's RAM-optimized instances address Marax's needs and help the company to reduce costs
- Managed Kubernetes is a new offering from DigitalOcean, which will help Marax drive greater application availability and scale
- Support from DigitalOcean helps developers and startups to scale and perform efficiently. It enables start-ups to focus more on the product and less on the cloud infrastructure
- A separate DevOps team is not required—every engineer on the team can be added to the cloud and can manage infrastructure independently
- Security is not a concern as managed DNS and Load Balancer allow developers to keep the 'Let's Encrypt' TLS certificates updated, which encrypts all connections to servers

"A friendly and well-structured user interface makes it easy for developers to start using the cloud. DigitalOcean's Hatch community is extremely responsive and helpful. They address queries and resolve issues quickly. The company also nurtures a big community of developers, who continuously share tips and trends to enhance cloud usage," says Gupta.

Marax has been able to reduce monthly cloud costs by approximately 30%. ■

NPCIL Malware: Is The Big Worry Justified?

The isolation of business systems and control systems are just assumed; not known. So, the worry is very, very real

By Shyamanuja Das

Last month, the incident of a malware hitting Nuclear Power Corporation of Indian Ltd (NPCIL)'s Kudankulam Nuclear Power Plant (KNPP) was all across media and social media.

The matter was politicized after Congress' Shashi Tharoor—incidentally, quite active on Twitter—appealed to the government to come clean on the matter and DMK's M K Stalin asked for a probe. As usual, social media was divided across ideological/political lines. Almost nine out of ten who joined the debate did not understand anything. From the rest, most were playing on others' ignorance. A few sane voices are not getting heard.

One of those voices is Pukhraj Singh, a cyber intelligence analyst, earlier involved with the setting up of the cyber defence operations center of the Indian government, who first spoke about it on Twitter and whose tweet was quoted by Shashi Tharoor to demand that the government 'owes us an explanation'.

"I just witnessed a casus belli in the Indian cyberspace and it sucks at every level," Singh tweeted, in a somewhat cryptic manner, way back on 7 September 2019.

Once other users started discussing it on Twitter, he tweeted again on 28 October, quoting his original tweet: "So, it's public now. Domain controller-level access at Kudankulam Nuclear Power Plant. The government was notified way back. Extremely mission-critical targets were hit."

What is significant is that Singh claimed that there were 'other targets', 'scarier than KNPP'. The government is largely silent on this and so is the media.

Next day he clarified that he did not discover the intrusion but a third party did that. He also claimed that he notified National Cyber Security Coordinator about this on 4 September 2019, a good three days before he tweeted about it. Later, in another tweet, he corrected the data: It was 3 September and not 4 September. That is a day earlier.

Confusion started when KNPP, a government agency, decided to play on words—the way some politicians and some businesses do—to take advantage of the ignorance

That is when Twitter went abuzz, Shashi Tharoor quoted him, asking the government to come clean and Twitter went abuzz. The first reaction that came from the authorities was a denial.

In an official statement, signed by R Ramadoss, Training Superintendent & Information Officer, KNPP said, "Some false information is being propagated on the social-media platform, electronic and print media with reference to the cyber-attack on Kudankulam Nuclear Power Plant."

"This is to clarify KNPP and other Indian Nuclear Power Plants Control are standalone and not connected to outside cyber network and Internet. Any cyber-attack on the Nuclear Power Plant Control System is not possible. Presently, KNPP Unit-1 and 2 are operating at 1000 MWe and 600 MWe respectively without any operational or safety concerns," it added.

That was the beginning of all confusion. While KNPP was (most probably) right in ascertaining that 'KNPP Unit-1 and 2 are operating at 1000 MWe and 600 MWe respectively without any operational or safety concerns,' it went a little overboard by claiming that 'any cyber-attack on the Nuclear Power Plant Control System is not possible.'

But that is not what made things confusing. Confusion started when KNPP, a government agency, decided to play on words—the way some politicians and some businesses do—to take advantage of the ignorance of the public and the journalists.

So, the next day when Nuclear Power Corporation of India Limited (NPCIL), admitted that identification of malware in NPCIL system is correct, media called it a U-turn.

In the war of words that followed, the slightly more-aware supporters of the government pointed out that there is nothing in the NPCIL statement that contradicts the earlier statement by

KNPP. While the malware information is correct, it 'did not' affect the plant operational system and only the office/business system.

"The matter was immediately investigated by the Department of Atomic Energy (DAE) specialists. The investigation revealed that the infected PC belonged to a user who was connected in the internet connected network used for administrative purposes. This is isolated from the critical internal network. The networks are being continuously monitored," the NPCIL statement clarified.

"Investigation also confirms that the plant systems are not affected," it reaffirmed.

This gives rise to multiple questions and doubts:

1.Why did the KNPP statement remain silent on the office PC that was affected, when social media was abuzz and instead called everything false information?

2. What changed between 28 October and 29 October 2019 for NPCIL to admit that indeed it was impacted, even though the same statement admitted that 'the matter was conveyed by the Indian Computer Emergency Response Team (CERT-In) when it was noticed by them on September 4, 2019."

3. How much can we rely on this assurance that the plant is not affected?

4. Why should a government agency try to play on the ignorance of the common man? It could have explained the difference between an office PC and the operational system. The Industrial Control Systems (ICS) and the business systems are usually isolated and the ICS in critical strategic infrastructure are rarely connected to public internet.

An ICS expert, Joe Slowik (@jfslowik) raised some pertinent points on

Dtrack: previously unknown spy-tool by Lazarus hits financial institutions and research centers

Published by Kaspersky on 23 September 2019

Kaspersky Global Research and Analysis Team have discovered a previously unknown spy tool, which had been spotted in Indian financial institutions and research centers. Called Dtrack, this spyware reportedly was created by the Lazarus group and is being used to upload and download files to victims' systems, record key strokes and conduct other actions typical of a malicious Remote Administration Tool (RAT).

In 2018, Kaspersky researchers discovered ATMDtrack – malware created to infiltrate Indian ATMs and steal customer card data. Following further investigation using the Kaspersky Attribution Engine and other tools, the researchers found more than 180 new malware samples that had code sequence similarities with the ATMDtrack, but at the same time were not aimed at ATMs. Instead, its list of functions defined it as spy tools, now known as Dtrack. Moreover, not only did the two strains share similarities with each other, but also with the 2013 DarkSeoul campaign, which was attributed to Lazarus – an infamous advanced persistence threat actor responsible for multiple cyberespionage and cyber sabotage operations.

Dtrack can be used as a RAT, giving threat actors complete control over infected devices. Criminals can then perform different operations, such as uploading and downloading files and executing key processes.

Entities targeted by threat actors using Dtrack RAT often have weak network security policies and password standards, while also failing to track traffic across the organization. If successfully implemented, the

spyware is able to list all available files and running processes, key logging, browser history and host IP addresses, including information about available networks and active connections.

The newly discovered malware is active and based on Kaspersky telemetry, and is still used in cyberattacks.

"Lazarus is a rather unusual nation state sponsored group. On one hand, as many other similar groups do, it focuses on conducting cyberespionage or sabotage operations. Yet on the other hand, it has also been found to influence attacks that are clearly aimed at stealing money. The latter is quite unique for such a high profile threat actor because generally, other actors do not have financial motivations in their operations," said Konstantin Zykov security researcher, Kaspersky Global Research and Analysis Team. "The vast amount of Dtrack samples we found demonstrate how Lazarus is one of the most active APT groups, constantly developing and evolving threats in a bid to affect large-scale industries. Their successful execution of Dtrack RAT proves that even when a threat seems to disappear, it can be resurrected in a different guise to attack new targets. Even if you are a research center, or a financial organization that operates solely in commercial sector with no government affiliates, you should still consider the possibility of being attacked by a sophisticated threat actor in your threat model and prepare respectively."

Dtrack Remote Administration Tool (RAT) is a cyber-espionage malware, an infamous advanced persistence threat actor responsible for multiple cyber-espionage and cyber-sabotage

Twitter. He questioned if assumption about the isolation of these two systems in India is there. In the US, the UK, Canada, Germany and France, "there's general confidence about network isolation between business and operational networks as both best practice and regulatory requirement - but does anyone know about India?" he asked. And if it is there in principle, he asked if its followed and enforced? India, anyway is known for great rules, with minimal enforcement.

And he sums up perfectly.

"On its face this looks 'bad', but lack of details and operational understanding means no one on the socials can accurately assess possible impacts and implications given very little info right now," he tweeted.

It comes back to where it started—whether you want to believe the control systems are completely isolated or they are not. If it is the latter, while NPCIL may still be right in saying that they are not affected right now, but the possibility of their getting affected is very real.

What is really worrying is that the type of malware and where it was found.

Dtrack Remote Administration Tool (RAT) is a known cyber-espionage malware from Lazarus Group, an infamous advanced persistence threat actor responsible for multiple cyber-espionage and cyber-sabotage operations. And it was found inside what should be the paragon of safety and security – a large nuclear plant of one of the few nuclear power nations in the world.

It is difficult to believe it was there to steal data from the employee payroll or office accounting system!

The Endnote

However, the incident will go down as one of the best things to happen if this sensitizes the government and that results in some real action.

Let's hope for the best...And I do not have hearts to complete the saying. ■

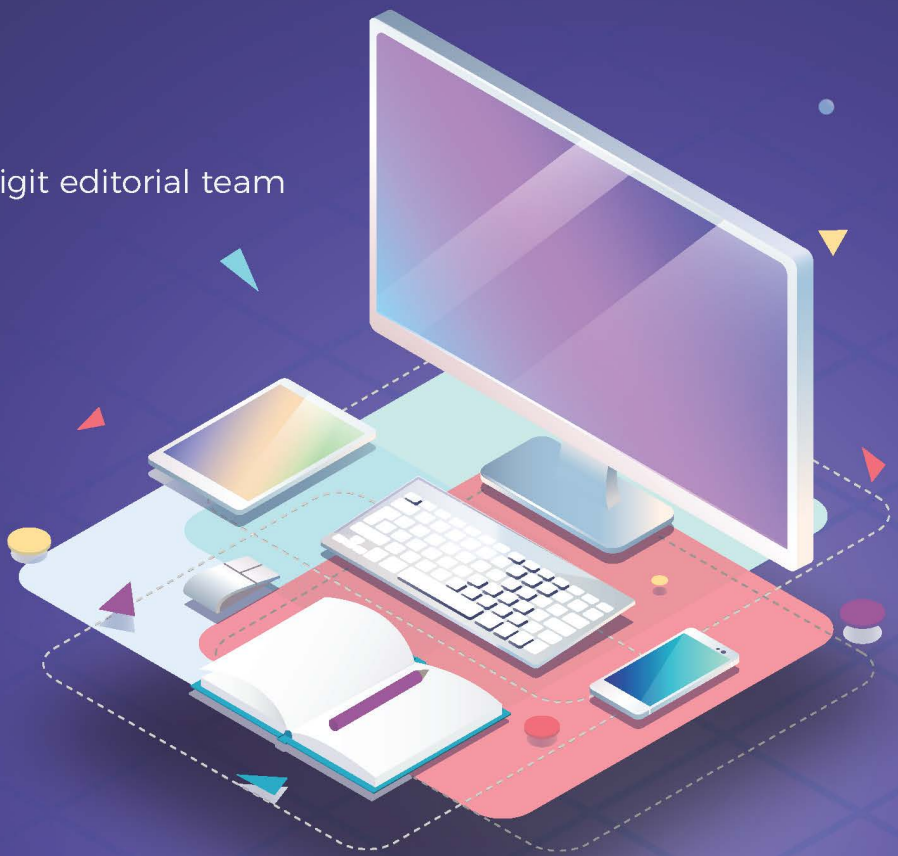
LAUNCHING

digit SQUAD

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

PKI's Role in Forging Digital Trust

Adopting and installing PKI has been known to offer significantly stronger security with better encryption methodology compared to password-based authentication

By Arvind Srinivasan

"Complexity is the worst enemy of security." When Bruce Schneier said this about 20 years ago, top cyber threats (nowadays) like phishing or 'Man in the Middle' attacks, were at a nascent stage. Adding fuel to the fire, recent escalations in cyber-crimes point to the fact that the threat index is on the rise and a full-fledged attack using these techniques can prove fatal to an organization's reputation, operations and everything in between and beyond.

To counter this malice, organizations must capitalize on two things. First, strengthening security infrastructure by adopting Public Key Infrastructure (PKI), and the other, fortifying 'Digital Trust' among its customers and safeguarding their interests while minimizing business risk.

Balancing security and trust factors as mentioned above needs a solution with a proven track record. PKI based security solutions have been popular among organizations due to the unbeatable track record for mission-critical enterprise applications. It is

built upon complex mathematical cryptographic functions designed to create, store, manage and send out authenticated digital certificates and their associated encryption keys.

How Security Landscape Changed with "Digital Trust"?

Disruption of services – leading to financial loss, damage to business reputation are some major business risk factors that enterprises must deal with during a confirmed cyber breach. Today, enterprises who deal with sensitive user and business data have realized that they can fortify digital trust at user, device, or server level. This is where PKI-based solutions can offer assurance and the much-needed immunity against breaches while mitigating business risks.

PKI can be easily integrated into a digital ecosystem made up of IoT devices; IoT-enabled networks, surveillance systems, and other mission-critical applications. PKI works this out by facilitating the secure exchange of data between end-users, connected devices, embedded systems, web servers or programs/applications addressing business risks and vulnerabilities which form the basis of digital trust.

How PKI Forges Digital Trust

Adopting and installing PKI has been known to offer significantly stronger security with better encryption methodology compared to password-based authentication. It also makes sure that below trust criterions are met:

- **Confidentiality:** PKI ensures the secrecy and privacy of data and guarantees that no one other than the expected parties can access the data.
- **Authentication:** PKI verifies the identity of entities or ensures that the persons with whom you are corresponding are who they say they are.
- **Integrity:** PKI ensures that data cannot be corrupted or modified, and transactions cannot be altered using digital signatures.

PKI can prevent 'Man in the Middle' attack from happening; shielding attackers at the primary level itself. The man in the "Middle" never gets the key to decrypt or modify any transaction, thereby reinforcing digital trust. PKI can alleviate breaches and weak links...

- **Non-Repudiation:** PKI ensures that data cannot be renounced, or a transaction denied.

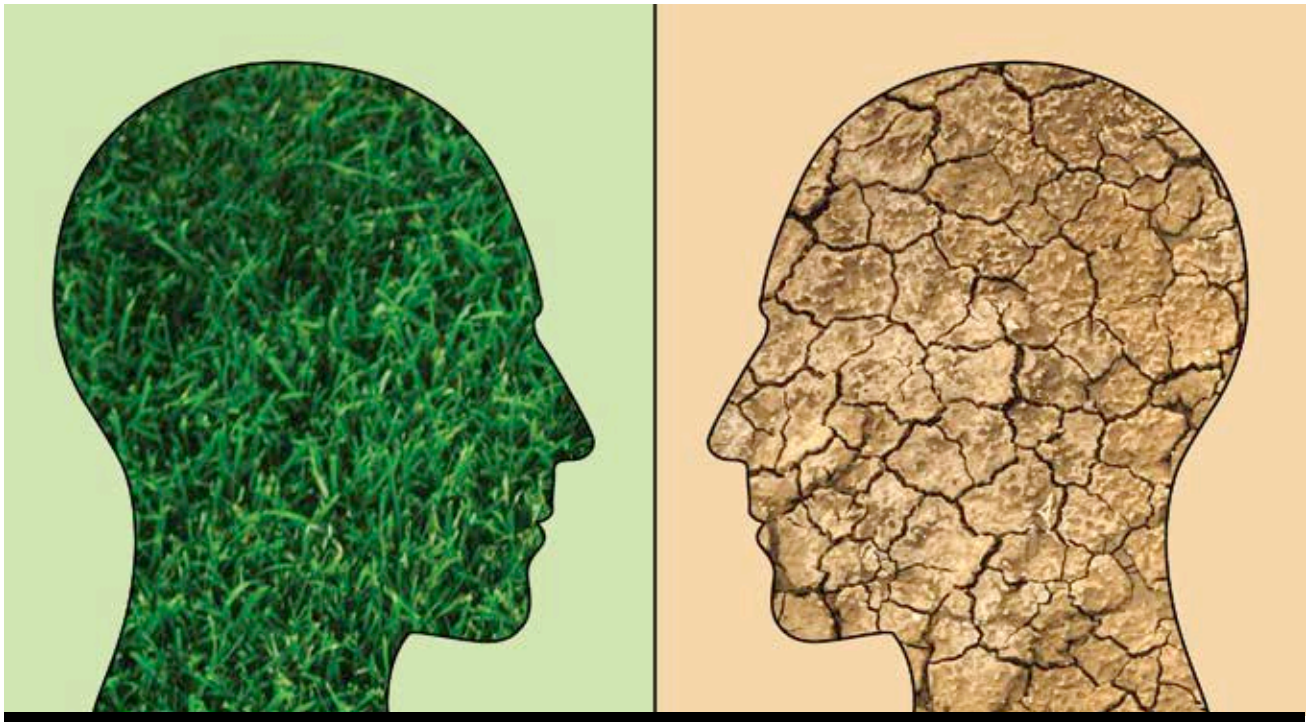
PKI Can End "Weak Links" in Your Network

Cybercriminals are always on the prowl to find new ways of breaching enterprise security infrastructure, especially password-based systems. Once they crack password, etc., the first layer of security, they are largely in the clear. If you are familiar with 'Man in the Middle' attack or MitM, PKI can prevent it from happening; shielding attackers at the primary level itself. The man in the "Middle" never gets the key to decrypt or modify any transaction, thereby reinforcing digital trust. PKI with the above-mentioned qualities can alleviate breaches and weak links through which cyber criminals create malicious tunnels into the enterprise network.

Your Enterprise is Never Too Late for Adopting PKI

The key to implementing a successful PKI integration lies in the way it is designed, which is keeping the organization's data infrastructure in mind. PKI is agile, which makes it apt for legacy systems and emerging technologies of today. Emerging technologies like IoT and Blockchain can leverage the PKI's capabilities to additionally fortify security around their existing infrastructure. PKI can offer effective security and digital trust keeping the complexity and diversity of today's corporate network. The list of advantages that PKI's scalable properties brings about to forge the element of "Digital Trust" is endless. ■

The author is SVP - Strategic - Global Initiatives, eMudhra



The Human Existential Crisis: AI Has The Potential To Tackle Climate Change

AI algorithms can help predict the right mixture of crops to plant to regenerate soil health and reduce fertilizer use

By Tuhin Banik

Climate change is the most important crisis the planet is facing today. Millions of people from all over the world took to the streets recently demanding urgent governmental action to help control the ongoing catastrophe and reverse the negative impact of climate change. We will need to marshal all our resources, including artificial intelligence to save our planet from peril. Some of the foremost minds in machine learning and artificial intelligence recently published a study where they outlined 13 crucial areas where machine learning can be used to mitigate the adverse effects of climate change. The recommendations they made were divided into three major categories – high leverage solutions, where machine learning can make a noticeable impact, long term solutions that will take at least a couple of decades to pay off, and finally, high risk pursuits, where the technology is either not mature enough or we don't know enough to effectively predict the consequences. Policy measures by the government should focus on implementing some of the high leverage solutions at scale to reduce our carbon footprint. Let us take a look at some of them that can make a significant difference:

Improve predictions on electricity needs – To deploy renewable energy in a more efficient way, utilities must be better able to predict energy

requirements, both in real-time and over a longer time period. There are plenty of algorithms that can already predict energy demands, and we can refine them further by considering climate patterns, local weather, and household energy usage. By making the algorithms more understandable, we can greatly assist utility operators interpret outputs and use the results to schedule when to switch over to renewable energy in the power grids.

Discover more energy efficient materials – Scientists are constantly looking for ways to harvest, store and utilize energy in a more efficient manner. However, the process of discovering or synthesizing new materials is slow and not very precise. Machine learning can help speed up the process of designing novel chemical compounds with energy efficient properties. For instance, it can help us design solar fuels that can capture and harness the Sun's energy more efficiently, identify materials that absorb carbon dioxide better and design structural materials that take a lot less carbon to manufacture. The day is not far when the latter would replace cement and steel, which will be a change for the better, as their production accounts for nearly 10% of greenhouse gas emissions.

Design energy efficient buildings – Intelligently designed control systems can drastically reduce the energy consumption of buildings. They can be programmed to take building occupancy, weather forecasts, and other miscellaneous environmental conditions so residents can adjust the cooling, heating, lighting and ventilation needs indoors. Smart building can also directly communicate with the electricity grid and reduce power usage if there is paucity in low-carbon power.

Help scale up precision agriculture – Monoculture currently dominates agricultural practice. It refers to the practice of growing one crop in a vast area. Adopting this approach is easy for farmers as they can deploy tractors and automated tools to manage the upkeep of their fields. However, it reduces the nutrient content of soil and hampers productivity over time. Consequently, farmers have to heavily rely on nitrogenous fertilizers that produce nitrous oxide, which is one of the most potent greenhouse gases. By deploying robots that use machine learning based software, farmers can manage a mixture of crops more efficiently, and AI algorithms can help predict the right mixture of crops to plant to regenerate soil health and reduce fertilizer use.

Improve the tracking of deforestation activity – Deforestation is a major contributor to the emission of greenhouse gases. However, the prevention of deforestation is a laborious on-ground manual process. Satellite imagery combined with computer vision technology can help us scan for the loss of green cover more efficiently and on a much larger scale. Sensors, if planted strategically on the ground, can be used in combination with algorithms to detect axe and chainsaw sounds. This will greatly help law enforcement officers detect and put an end to illegal deforestation activity.

For people in the field of machine learning, this is an exciting time to use their skills for the greater good. Identify opportunities in your community and outside where you can use your skills in any way to help build a low carbon economy, and contribute to the global fight against climate change. ■

Farmers have to heavily rely on nitrogenous fertilizers that produce nitrous oxide, one of the most potent greenhouse gases. By deploying robots that use machine learning based software, farmers can manage a mixture of crops and AI algorithms can help predict the right mixture...

The author is Founder, Thatware LLP

Agile Security - A Reality In Today's World

Security professionals can maximize security for containerized applications with a unique combination of positive and negative security models for application protection in service mesh

By Nikhil Taneja

Businesses are looking to optimize and accelerate their Software Development Lifecycle (SDLC), in order to improve their operational efficiency and gain a competitive edge.

Service mesh is the popular architecture where monolithic applications are broken down into microservices, becoming the common delivery model providing for better agility, elasticity and scale. Companies that deploy service mesh architecture require advanced automation and orchestration tools to help them achieve these business goals (agility, elasticity, and scale) and assemble an ecosystem that supports continuous deployment.

Such orchestration tools offer automated container deployment, scaling and

management, time code scanning, provisioning, testing and even security in the CI/CD pipeline. The most popular orchestration tool is Kubernetes. It is so broadly used, that each public cloud vendor has introduced a special Kubernetes edition.

Naturally, these benefits drive the rapid adoption of the above model, with the ultimate goal of continuous deployment. Even if an application is changed multiple times a day, each version must go through the full SDLC phases before being pushed into production – with no delays and no human intervention, at all. If security doesn't run at the same speed, it is usually left behind.

Normally, enterprises are forced to choose between agility and security. Most put agility first and try to retrofit security solutions into their deployments. But it's worth noting that digital transformation doesn't just come with new technologies; it also forces structural changes and adjustments of business processes.

Naturally, because it gives more decision-making power to those who understand, choose and implement the emerging solutions, DevOps have a growing influence on information security related decisions and eventually, the overall application security posture of their company.

As Everything is Moving Fast, How Can Businesses Be Both Agile and Secure?

Unfortunately, emerging technologies are just that—emerging—and they do not come with best practices. Companies still look for the proverbial yellow brick road to secure microservices and containerized applications. What might that look like? Market leading application security that also provides advanced automation, auto-scale and elasticity required by today's DevOps and Security teams. But often, the first line of defense is a WAF.

Can a WAF be Agile?

WAFs are long known as showstoppers – they are slow, inaccurate, require a lot of tuning, exception handling and manual labor to maintain. Generating false positives and hurting the user experience, WAFs are by far the least favorite solution for information security teams. Can such an ancient animal adjust to the new ecosystem?

Normally, enterprises are forced to choose between agility and security. Most put agility first and try to retrofit security solutions into their deployments

Yes, it Can!

If organizations require agility first and foremost, then security must fit into that automated SDLC without disrupting continuous deployment. However, organizations need more than just a "good enough" security solution. Their data is at stake. They require comprehensive protection. Radware invested significant R&D efforts to solve this problem. The emphasis focused on finding the required level of automation, flexibility and elasticity.

Kubernetes WAF features many integration options into the CI/CD pipeline. For example, it is fully controlled by Kubernetes, so application security grows and scales with Kubernetes pods, including learned policies and configuration settings.

What's more, visibility to both DevSecOps + Security teams via integration with common tools and platforms (like Grafana, Prometheus, etc.) is critical, as is a light footprint (an enforcement point in front of each pod while management, analytics and learning engine are run separately within the environment).

Lastly, and perhaps most importantly, security policies should be automatically generated and tuned. This can be accomplished by using machine learning with a unique auto policy-generation engine that studies the application/ microservice structure, analyzes potential threats and builds a security policy that is later adjusted whenever a change is introduced to the application.

And There You Have It: Agile Security!

As for security folks – you can maximize security for containerized applications with a unique combination of positive and negative security models for application protection in service mesh. ■

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

How To Create A Cyber-Aware Workforce Using Non-Traditional Training Techniques

There are many scientific benefits to some non-traditional training techniques such as reduction of cognitive load, leaving learners feeling more engaged and increasing their level of information retention

By Rajesh Maurya

Much has been made about the cybersecurity skills gap, and for good reason. There is a scarcity of cybersecurity professionals worldwide, which makes networks and those who depend on them—which is almost everyone—less safe. This is compounded by the fact that humans continue to be the weakest link in an organization's cybersecurity posture. There is an insufficient number of professionals to keep networks secure, and there is a general lack of cybersecurity awareness by employees making basic mistakes that create greater cyber risk.

The Benefits of Non-Traditional Training

The traditional view of training is of people sitting in a classroom for several hours or days with an instructor or facilitator at the front of the room. Or of sitting in front of a computer working through many modules of a self-pace training course. While these methods of training can be quite effective, the field of training and education has evolved considerably over the last several years.

There are many forms of less traditional training methods that have proven to be very effective and can address challenges CISOs are facing in building a truly cyber aware workforce. Implementing many of these non-traditional techniques means that employees are away from their workplace far less (in some cases not at all) and transforms the learning experience from an isolated event where the learner "consumes training content" to a culture of continuous learning where employees are "active participants" in a more informal, social, interest-driven learning process.

There are many scientific benefits to some non-traditional training techniques such as reduction of cognitive load leaving learners feeling more engaged and increasing the levels of information retention. The scientific benefits are beyond the scope of this

post, but there is no shortage of scientific data available to anyone online. Examples of non-traditional training techniques include:

■ **Job Aids:** As stated above, training doesn't always need to be employees sitting in a classroom. There are many times when employees need to perform tasks that are exceptions to their day-to-day routine and that can be quite complicated and unfamiliar. Often these tasks can be learned far more effectively through the use of job aids. A good example of this is when an employee receives an email that could be malicious. Rather than wading through a large training manual or trying to remember the specific characteristics of malicious emails that were discussed in a previous class, an employee can reach for a job aid. This type of job aid could be as simple as a two-sided laminated sheet with one side describing the characteristics of various malicious emails and the other side with simple flow charts of what to do. This is essentially 'Just-in-Time' learning that will soon become second nature to the employee.

■ **Microlearning:** Microlearning is a general concept of providing relatively small chunks of learning to participants where and when it is appropriate. Microlearning content can be delivered in a variety of ways ranging from modern learning management systems (LMS) that push microlearning content to users. Or it can be through less formal means such as quizzes integrated into regular news letters or informal activities. Microlearning is an ongoing trend that meets the particular needs of today's fast-moving organizations and their employees. While it is a general concept that applies to a number of techniques, Microlearning is best suited for skills-based learning which is quite applicable to cybersecurity skills and awareness. With the landscape changing so often, microlearning can be delivered regularly to reinforce security topics and required skills, increasing the odds of retention and compliance.

■ **Gamification:** Gamification is a technique using elements comprised of video game design in learning environments. The goal of gamification is to engage learners through familiar fun activities and in some cases create a competitive and or social environment. By gaining points, elevating their status level, getting to the top of a leaderboard or one of many other gaming techniques, users are inspired to continue learning. Gamification of learning can be implemented in a number of ways and to a number of degrees. It can be as simple as awarding points as people participate in ongoing microlearning activities, or more complex live in-person "capture-the-flag" competitions. From a cybersecurity awareness perspective, gamification of learning could be implemented in conjunction with MIS teams sending out simulated phishing attacks and awarding points to employees who avoid the attacks and can identify various characteristics. The Fortinet XPerts Academy event in Latin America is a good example of gamification being used in a much more extensive manner to create excitement and engagement before a training event even starts. Take a look at the challenge video sent to registered participants.

■ **Digital Badging:** Digital badges are defined as "a validated symbol or indicator of an accomplishment, skill, quality or interest". While not a training technique itself, digital badging can be a great tool to motivate behavior and engage learners by recognizing achievement. Digital badging can also be used as a mechanism to communicate a person's status or membership within a community. In fact, digital badging is quickly becoming an alternative to traditional technical certification designations that often require significant time and financial investment by individuals. In 2011 the whitepaper "An Open Badge System Framework" by Peer 2 Peer University and The Mozilla Foundation became the catalyst for what has become an effective network of open digital badging systems that allow individuals to share their badges broadly across the internet with peers, credentialing bodies, potential employers and others. This can be a great enabler for CISOs and HR departments wanting to assess skills and knowledge of potential new hires into an organization. It can also be a great tool for internal compliance teams to easily measure and report on critical cybersecurity awareness of the general employee population.

■ **Awareness Campaigns:** While not as technological as gamification or digital badging, an often overlooked method of training is leveraging existing awareness campaigns. These campaigns can be focused specifically on a training initiative such as cybersecurity awareness, or could be larger campaigns that are well aligned with your learning objectives – such as Cybersecurity Awareness Month. They can be internal campaigns or external campaigns that typically provide a significant number of resources and support. The Association for Talent Development for example promotes an Employee Learning Week each year, citing a growing skills gap and the need to remain competitive in today's global economy.

Cybersecurity remains a primary concern for all organizations and cybersecurity awareness training needs to be part of any successful strategy to keep networks and data safe. The BYOD, work-anywhere culture increases risk, but it also provides greater opportunity to train employees on good cybersecurity practices using a variety of non-traditional training techniques. By evolving your organization's training strategy to include a variety of non-traditional techniques for your cybersecurity needs, you have the potential to do more than build a Cyber-Aware Workforce, you have the potential to change the overall learning culture of your organization and become a true Learning Organization. ■

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

Unaccounted Authentication Identities Or Stolen Privileged Credentials?

Six reasons to take control of your orphaned encryption keys

By Shwetha Sankari

A close analysis of the cybersecurity attacks of the past shows that, in most cases, the head of the cyber kill chain is formed by some kind of privilege abuse. In fact, Forrester estimates that compromised privileged credentials play a role in at least 80% of data breaches. This is the reason Privileged Access Management (PAM) has gained so much attention over the past few years. With securing and managing access to business-critical systems at its core, PAM aims to provide enterprises with a centralized, automated mechanism to regulate access to super-user accounts. PAM solutions ideally do this by facilitating end-to-end management of the privileged identities that grant access to these accounts.

However, the scope of privileged access security is often misconceived and restricted to securing and managing root account passwords alone. Passwords, beyond a doubt, are noteworthy privileged access credentials. But the constant evolution of technology and expanding cybersecurity perimeter calls for enterprises to take a closer look at the other avenues of privileged access, especially encryption keys—which despite serving as access credentials for huge volumes of privileged accounts, are often ignored.

This article lays focus on the importance encryption key management—why enforcing SSH key and SSL certificate management is vital, and how by doing so, you can effectively bridge the gaps in your enterprise privileged access security strategy.

1. Uncontrolled numbers of SSH keys trigger trust-based attacks

The average organization houses over 23,000 keys and certificates many of which grant sweeping access to root accounts, says a Ponemon survey. Also, a recent report about the Impact of Unsecured Digital Identities states that 71% of the respondents did not have any idea about the number of keys or the extent of their access within the organization. Without a centralized key management approach, anybody in the network can create or duplicate any number of keys. These keys are often randomly generated as needed and are soon forgotten once the task they are associated with is done. Malicious insiders can take advantage of this massive ocean of orphaned SSH keys to impersonate admins, hide comfortably using encryption, and take complete control of target systems.

2. Static keys create permanent backdoors

Enterprises should periodically rotate their SSH keys to avoid privilege abuse, but huge volumes of unmanaged SSH keys make key rotation an intimidating task for IT administrators. Moreover, due to a lack of proper visibility on which keys can access what, there is widespread apprehension about rotating keys in fear of accidentally blocking access to critical systems. This leads to a surge of static SSH keys, which have the potential to function as permanent backdoors.

3. Unintentional key duplication increases the chance of privilege abuse

For the sake of efficiency, SSH keys are often duplicated and circulated among various employees in an organization. Such unintended key duplication creates a many-to-many key-user relationship, which highly increases the possibility of privilege abuse. This also makes remediation a challenge since administrators have to spend a good amount of time revoking keys to untangle the existing relationships before creating and deploying fresh, dedicated key pairs.

Without a centralized key management approach, anybody in the network can create or duplicate any number of keys... Malicious insiders can take advantage of this massive ocean of orphaned SSH keys

4. Failed SSL certificate renewals hurt your brand's credibility

SSL certificates, unlike keys, have a set expiration date. Failing to renew SSL certificates on time can have huge implications on website owners as well as end users. Browsers don't trust websites with expired SSL certificates; they throw security error messages when end users try to access such sites. One expired SSL certificate can drive away potential customers in an instant, or worse, lead to personal data theft for site visitors.

5. Improper SSL implementations put businesses at risk

Many businesses rely completely on SSL for internet security, but they often don't realize that a mere implementation of SSL in their network is not enough to eliminate security threats. SSL certificates need to be thoroughly examined for configuration vulnerabilities after they are installed. When ignored, these vulnerabilities act as security loopholes which cybercriminals exploit to manipulate SSL traffic and launch Man-in-the-Middle (MITM) attacks.

6. Weak certificate signatures go unheeded

The degree of security provided by any SSL certificate depends on the strength of the hashing algorithm used to sign the certificate. Weak certificate signatures make them vulnerable to collision attacks. Cybercriminals exploit such vulnerabilities to launch MITM attacks and eavesdrop on communication between users and web servers. Organizations need to isolate certificates that bear weak signatures and replace them with fresh certificates containing stronger signatures.

Bridging the gaps in your PAM strategy

All the above scenarios highlight how important it is to widen the scope of your privileged access security strategy beyond password management. Even with an unyielding password manager in place, cybercriminals have plenty of room to circumvent security controls and gain access to superuser accounts by exploiting various unmanaged authentication identities, including SSH keys and SSL certificates. Discovering and bringing all such identities that are capable of granting privileged access under one roof is one important step enterprises should take to bridge gaps in their privileged access security strategy. For, today's unaccounted authentication identities could become tomorrow's stolen privileged credentials! ■

The author is Product Consultant, ManageEngine

5G To Help Customer Acquisition And Generate New Revenue Streams: Study

90% of enterprises are actively investigating business cases, defining use cases with ecosystem partners or defining service portfolios using 5G technology

Over 50% enterprises believe 5G will help customer acquisition and generate new revenue streams, according to Infosys Knowledge Institute's market research titled, 'State of 5G – The Road Ahead'. The research was aimed at gathering insights around the current state of 5G adoption and identifying current and future initiatives that can serve as a guide for business and technology leaders across enterprises in their 5G digital transformation journey.

For this research, Infosys surveyed 850 senior executives representing firms from 12 industries, with annual revenues over USD 1 billion across US, Europe, UK, Australia and New Zealand. The study gathered empirical evidence to show how mass machine communication is expected to be the most transformed application with 5G and why data

security emerges as the most critical barrier to its adoption.

Key findings of the survey include:

- A staggering 90% of the respondents are either actively investigating 5G business cases or defining various use cases and service portfolios with ecosystem partners.
- Nearly 60% of respondents mentioned cost and effectiveness as the primary criteria for use case adoption, while 57% of surveyed enterprises are looking at 5G for new revenue streams.
- Over 50% of enterprises are looking for 5G use cases that can help them disrupt the market or drive their brand forward
- Data security (59%), finding the right talent (57%), and device readiness (57%) were identified as key barriers in 5G adoption.
  - Industry wise, Energy and Utilities call out Integration while Manufacturing mentions virtualized 5G core deployment as key challenges
  - Maintenance of the new technology (47%) and defining a roadmap for AI and ML technology advancements (33%) emerged as key challenges post implementation
- Nearly 50% enterprises firmly believe that system integrators play a vital role in 5G deployment.
- 50% respondents cited that mass machine communication is expected to undergo a major transformation, followed by ultra-reliable and low latency services (48%) and enhanced cellular broadband (43%).
- State of 5G across industries:
  - Consumer Retail and Logistics (CRL) and Energy and Utilities (E&U) industries are leaders in 5G strategy with experiments around In-Store Experience and Smart Grids respectively. There is also traction in interactive experiences around media delivery, smart spaces, and remote healthcare.
  - Telecom industry is driving more use case experimentation (57%) that can help them disrupt the market.
  - Supply side industries have migrated beyond the business case stage, focusing more on prototyping. On the other hand, industries on the demand side are driven by the cautious nature of users while contemplating business cases.
- While standards organizations are seen as the preferred partners in 5G evolution among nearly 50% respondents, understanding of 5G and seamless transitioning capability were called out as the key partner selection criteria.

Nearly 60% of respondents mentioned cost and effectiveness as the primary criteria for use case adoption, while 57% are looking at 5G for new revenue streams... Over 50% are looking for 5G use cases that can help them disrupt the market or drive their brand forward

Nitesh Bansal, Senior Vice President and Global Head, Engineering Services, Infosys said, "5G holds significant transformation potential for both network providers and enterprises that will consume it. For network providers there are significant opportunities for network virtualization, AI and automation, while considerably lowering associated costs and enhancing delivery of network-based services. For enterprises, on the other hand it unlocks significant value with the addition of use cases that were not possible without low latency and high bandwidth network coverage. Through our research, 'State of 5G – The Road Ahead', we are looking to present a comprehensive view of the adoption and barriers in implementing 5G. The research also highlights relevant use cases that will serve as a ready reckoner for businesses looking to explore new opportunities in the 5G space." ■

More And More Organizations Becoming "Intelligent" With Growing IoT Investments: Study

A record 61% of enterprises worldwide are on the path to becoming "intelligent," compared to only 49% in 2018

A record 61% of enterprises worldwide are on the path to becoming "intelligent," compared to only 49% in 2018, according to Zebra Technologies Corporation's third annual *Intelligent Enterprise Index*.

This global survey analyzes the extent to which companies connect the physical and digital worlds to drive innovation through real-time guidance, data-powered environments and collaborative mobile workflows. Their "Intelligent Enterprise" Index scores are calculated using 11 criteria that include Internet of Things (IoT) vision, adoption, data management, intelligent analysis and more.

Based on these criteria and driven by an overwhelming pressure to improve the customer experience, retail organizations have gained the most momentum in the last 12 months, graduating from the bottom of the 2018 vertical Index rankings to nearly the top of the 2019 list, second only to Healthcare.

The number of companies defined as truly "intelligent enterprises" by achieving a score of 75 points or greater on the Index has also risen year over year. 17% of organizations with at least 250 employees crossed

this threshold in 2019 versus only 11% in 2018. Interestingly, 37% of surveyed small to medium-sized businesses (SMBs) with 50-249 employees scored 75 points or greater on the Index, indicating SMBs with an IoT vision are in many cases more "intelligent" than large enterprises.

"When we launched the Intelligent Enterprise Index three years ago, many enterprises were trying to understand where and how IoT solutions could be best applied within their unique business environments," said Drew Ehlers, Global Futurist, Zebra Technologies. "We now see more urgency to improve operational visibility and facilitate the delivery of actionable intelligence all the way to the edge of the enterprise. I believe that is why enterprises are now demonstrating a much greater commitment to executing their IoT plans and why we'll likely see a surge in investments over the next few years."

"With the continued adoption of mobility and IoT, the edge of enterprise operations is becoming increasingly connected. This unprecedented, growing level of connectivity is generating vast amounts of actionable data about processes and assets that can be leveraged to transform workflows to improve business performance and outcomes. As a breakthrough data intelligence platform that combines IoT end-point connectivity, configuration management, data transport, data storage, analytics and machine learning into one platform, Zebra's Savanna turns raw data into actionable insights for businesses to deliver new levels of service, productivity and profitability," said Deep Agarwal, Regional Sales Director of India, Zebra Technologies.

Some key Index findings include:

- **The pace of IoT adoption is picking up, leading to increasingly greater intelligence levels.** The cumulative Intelligent Enterprise Index score continues to grow as more companies move from exploratory to deployment phases of their journeys, with the 2019 score topping out at 61.5 points. This represents a nearly 6-point increase from 2018, driven largely by the increased "intelligence" gains of retail and transportation & logistics (T&L) organizations. It is also a +9-point gain from 2017, the first year the Index was conducted. Further, 74% of APAC organizations have an IoT vision with plans to execute it, of which 55% have already implemented while up to 43% are planning to implement it within the next 1-3 years.

- **Continued growth in IoT solutions and other data-driven technology platform investments.** In 2019, the average global enterprise spend was USD 6.4 million, representing a 39% year-over-year increase. 86% of enterprises expect this number to grow in the next 1-2 years, with over half of respondents expecting to increase their investments by 21-50+%. Up to 92% of APAC organizations expect their investments in IoT and mobility to increase over the next 1-2 years.
- **Intelligence-driven solution deployments have broadened quite significantly.** 46% of study respondents are currently implementing their IoT solutions on a company-wide level, an increase from 38% in 2018. Another 32% expect to soon move toward regional deployments.
- **With security a top priority, enterprises are committing more resources to continuous data system monitoring.** 62% of enterprises are now constantly monitoring their IoT security to ensure system integrity and data privacy. That is a 4-percentage point gain year-over-year and a 13-percentage point increase from 2017. At that time, only 49% had a constant security monitoring protocol with 47% periodically monitoring their systems. Up to 70% of APAC organizations are constantly monitoring their IoT security to ensure that their system integrity and privacy are not compromised.
- **Enterprises are shifting to a single partner "intelligent" solution ecosystem.** Nearly half (49%) of study respondents indicate they now rely on a single strategic partner to manage their entire "intelligence" solution, including components and services provided by third parties.
- **Surveyed SMBs score higher on the Index than large companies (64.5 points vs 61.5 points).** This higher score is based on findings such as SMB respondents indicating their enterprises are more likely to have an IoT vision and are executing on the plan (69% vs 62%). ■

Inefficient Incident Response To Email Attacks Costing Businesses Billions: Study

Attacks often have time to spread and cause more damage

Inefficient incident response to email attacks is costing businesses billions in losses every year. For many organizations, finding, identifying and removing email threats is a slow and manual process that takes too long and uses too many resources. As a result, attacks often have time to spread and cause more damage.

In a recent survey, Barracuda researchers found that, on average, a business takes three and a half hours (212 minutes) to remediate an attack. In fact, 11% of organizations spend more than six hours on investigation and remediation.

Here's a closer look at why manual incident response is inefficient, along with some solutions to help every business identify and remediate attacks more quickly.

Highlighted Threat

Inefficient incident response – Suspicious emails need to be identified and remediated quickly, before they spread across the organization and cause further damage. After all, in most phishing campaigns, it takes 16

minutes for someone to click on a malicious link. With manual incident response, however, it takes about three and a half hours for organizations to respond. In many cases, by that time, the attack has spread further, requiring additional investigation and remediation.

Fast and automated incident response is more important than ever, considering spear-phishing attacks designed to evade email security are on the rise. For example, business email compromise attacks, which include no malicious links or attachments, have been shockingly effective; in the last three years, these attacks have resulted in losses of USD 26 billion.

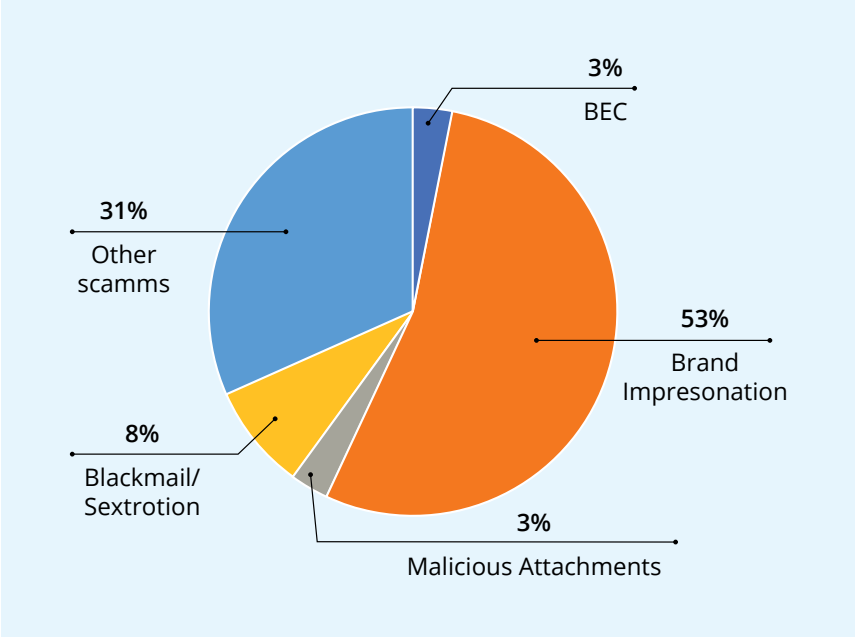
The Details

Barracuda researchers looked at the results of email threat scans of 383,790 mailboxes across 654 organizations over a 30-day period. They used the Barracuda Email Threat Scanner, a free tool that organizations can use to analyze their Office 365 environment and detect threats that got past their email gateway.

The scans conducted in this 30-day period identified nearly 500,000 malicious messages in these inboxes. On average, each organization had more than 700 malicious emails that users could access anytime.

How long would it take you to identify, investigate, and remediate all these malicious messages? At 3.5 hours of clean up per campaign, it would take days, if not weeks, to clean up and make sure that many malicious messages were removed.

In addition to these attacks that are already in your mailboxes, users report suspicious messages to IT every day. Based on data from Barracuda customers, a typical organization responds to around five email-related security incidents each day. With an average of 3.5 hours to respond to each incident, it takes more than 17 hours, or the equivalent of two full-time employees, to respond to what's being reported each day. That's time that could be spent on more proactive security measures, such as training employees, managing security patches, or investigating delivered mail for malicious content, which will help them stay ahead of attackers.



How You Can Improve Incident Response Time?

Organizations rarely have this kind of time and resources, so not all incidents are handled according to best practices. Often, IT departments need to prioritize which malicious messages need to be addressed first, leaving organizations, users, and data exposed.

This is where automated incidence response can help. Barracuda research shows that, with automated incident response, you can reduce your response time by 95% on average. For example, for 78% of our customers, incident response now takes less than 10 minutes. That means the five incidents reported by users each day would take less than an hour to remediate.

Automated incident response solutions let you easily identify all internal users who have received a malicious email and remove all instances of it. You can also automatically deliver alerts to affected users to warn them about the threat or provide other instructions.

Improving incident response time makes organizations more secure, helps limit damage, and saves valuable time and resources for IT teams.

Here are three steps you can take to improve incident response:

1. **Assess email vulnerabilities** - Scan your organization's inboxes to find malicious email and social engineering attacks that your email gateway missed. This will help you understand the vulnerabilities that exist in your email system and the scope of what needs to be investigated and remediated.
2. **Add spear-phishing protection** - Introducing an AI-based protection against phishing and account takeover will help you block these types of threats more effectively and stay ahead of attackers by using artificial intelligence to look for anomalies in real time.
3. **Automate incident response** - An automated incident response solution will help you quickly clean up any threats you found in users' inboxes during the email scan and make remediation more efficient for all messages going forward. ■

Major Online Marketplaces And Social Media Platforms To Support Cryptocurrency Payments By 2020: Gartner

50% of people with a smartphone but without a bank account will use a mobile-accessible cryptocurrency account, according to Gartner

50% of people with a smartphone but without a bank account will use a mobile-accessible cryptocurrency account, according to Gartner. This is among the top strategic predictions for 2020 and beyond, which examine how the human condition is being challenged as technology creates varied and ever-changing expectations of humans.

Top 10 Strategic Predictions for 2020 and Beyond

By 2023, the number of people with disabilities employed will triple due to AI and emerging technologies, reducing barriers to access.

"People with disabilities constitute an untapped pool of critically skilled talent," said Daryl Plummer, distinguished vice president and Gartner Fellow. "Artificial intelligence (AI), augmented reality (AR), virtual reality (VR) and other emerging technologies have made work more accessible for employees with disabilities. Organizations that actively employ people with disabilities will not only cultivate goodwill from their communities, but also see 89% higher retention rates, a 72% increase in employee productivity, and a 29% increase in profitability."

By 2024, AI identification of emotions will influence more than half of the online advertisements you see.
Artificial emotional intelligence (AEI) is the next frontier for AI development, especially for companies hoping to detect emotions in order to influence buying decisions. 28% of marketers ranked AI and machine learning (ML) among the top three technologies that will drive future marketing impact, and 87% of marketing organizations are currently pursuing some level of personalization, according to Gartner. Computer vision, which allows AI to identify and interpret physical environments, is one of the key technologies used for emotion recognition and has been ranked by Gartner as one of the most important technologies in the next three to five years.

Through 2023, 30% of IT organizations will extend BYOD policies with "bring your own enhancement" (BYOE) to address augmented humans in the workforce.
The concept of augmented workers has gained traction in social media conversations in 2019 due to advancements in wearable technology. Wearables are driving workplace productivity and safety across most verticals, including automotive, oil and gas, retail and healthcare. Although wearables are only one example of physical augmentations available today, humans will look to additional physical augmentations.

By 2025, 50% of people with a smartphone but without a bank account will use a mobile-accessible cryptocurrency account.
Major online marketplaces and social media platforms will start supporting cryptocurrency payments by the end of next year. At least half the globe's citizens who do not use a bank account will instead use these new mobile-enabled cryptocurrency account services offered by global digital platforms by 2025. This will open trading opportunities for buyers and sellers in growing economies like sub-Saharan Africa and Asia/Pacific.

By 2023, a self-regulating association for oversight of AI and machine learning designers will be established in at least four of the G7 countries.
Public demand for protection from the consequences of malfunctioning algorithms will in turn produce pressure to assign legal liability for the harmful consequences of algorithm failure. The immediate impact of regulation of process will be to increase cycle times for AI and ML algorithm development and deployment. Enterprises can also expect to spend more for training and certification for practitioners and documentation of processes, as well as higher salaries for certified personnel.

By 2023, 40% of professional workers will orchestrate their business application experiences and capabilities like they do their music streaming experience.
The human desire to have a work environment that is similar to their personal environment continues to rise — one where they can assemble their own applications to meet job and personal requirements in a self-service fashion. The consumerization of technology and introduction of new applications have elevated the expectations of employees to what is possible from their business applications.

By 2023, up to 30% of world news and video content will be authenticated as real by blockchain countering deep fake technology.
Fake news represents deliberate disinformation, such as propaganda that is presented to viewers as real news. Its rapid proliferation in recent years can be attributed to bot-controlled accounts on social media, attracting more viewers than authentic news and manipulating human intake of information.

Through 2021, digital transformation initiatives will take large traditional enterprises on average twice as long and cost twice as much as anticipated.
Business leaders' expectations for revenue growth are unlikely to be realized from digital optimization strategies, due to the cost of technology modernization and the unanticipated costs of simplifying operational interdependencies. Such operational complexity also impedes the pace of change along with the degree of innovation and adaptability required to operate as a digital business.

By 2023, individual activities will be tracked digitally by an "Internet of Behavior" to influence benefit and service eligibility for 40% of people worldwide.
Through facial recognition, location tracking and big data, organizations are starting to monitor individual behavior and link that behavior to other digital actions, like buying a train ticket. The Internet of Things (IoT) – where physical things are directed to do a certain thing based on a set of observed operating parameters relative to a desired set of operating parameters — is now being extended to people, known as the Internet of Behavior (IoB).

By 2024, the World Health Organization will identify online shopping as an addictive disorder, as millions abuse digital commerce and encounter financial stress.
Consumer spending via digital commerce platforms will continue to grow over 10% year over year through 2022. The ease of online shopping will cause financial stress for millions of people, as online retailers increasingly use AI and personalization to effectively target consumers and prompt them to spend discretionary income that they do not have. The resulting debt and personal bankruptcies will cause depression and other health concerns caused by stress. ■

Double Scoop

Two times
the revelation

Mehdihasan Naqvi

Head - IT
Otis Elevator Company (India)

A BOOK I LOVE READING

'Good to Great' by Jim Collins

MY PEER IN THE IT COMMUNITY

Md. Tariq Nadeem, Head - GST, Goods & Services Tax Network

MY FAVORITE SINGER

Mohammed Rafi

A FESTIVAL WHICH I ENJOY THE MOST

Eid

MY TECH IDOL

Bill Gates

MY FAVORITE SPORT

Cricket

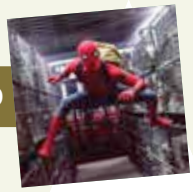
Md. Tariq Nadeem

Head - GST
Goods & Services Tax Network

MY FAVORITE CUISINE

Chinese

MY FAVORITE SUPERHERO



Spiderman

A TECH EVENT I RECENTLY ATTENDED

Oracle SQL Event at the Taj Delhi in October 2019

A TECH SHOW I LOVE WATCHING

Gadget Guru

MY FAVORITE DRESS

Business Formals

डिजिट
अब हिंदी में

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

digit.in
NOW IN HINDI

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

डिजिट

DATA CENTERS DESERVE

PERFORMANCE. RELIABILITY. CONSISTENCY.

Kingston TECHNOLOGY

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)

nvm EXPRESS | AES-256 ENCRYPTION | TAA COMPLIANT

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 IO Delivery

Enterprise Solid-State Drives (SSD)

Incredible Speeds With Full Security Suite.

Server Memory

Accelerate Performance