Insight | Pg 21
Application Security in a Multi-Cloud World

Insight | Pg 34
Five Most Largest and Famous DDoS Attacks in History

ITNEXT
FOR THE NEXT GENERATION OF CIOs

2021
THE YEAR OF HOPE

Eight adjustments enterprise IT managers should bring in based on the learnings from 2020

January 2021 | ₹100 | Volume 11 | Issue 10 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

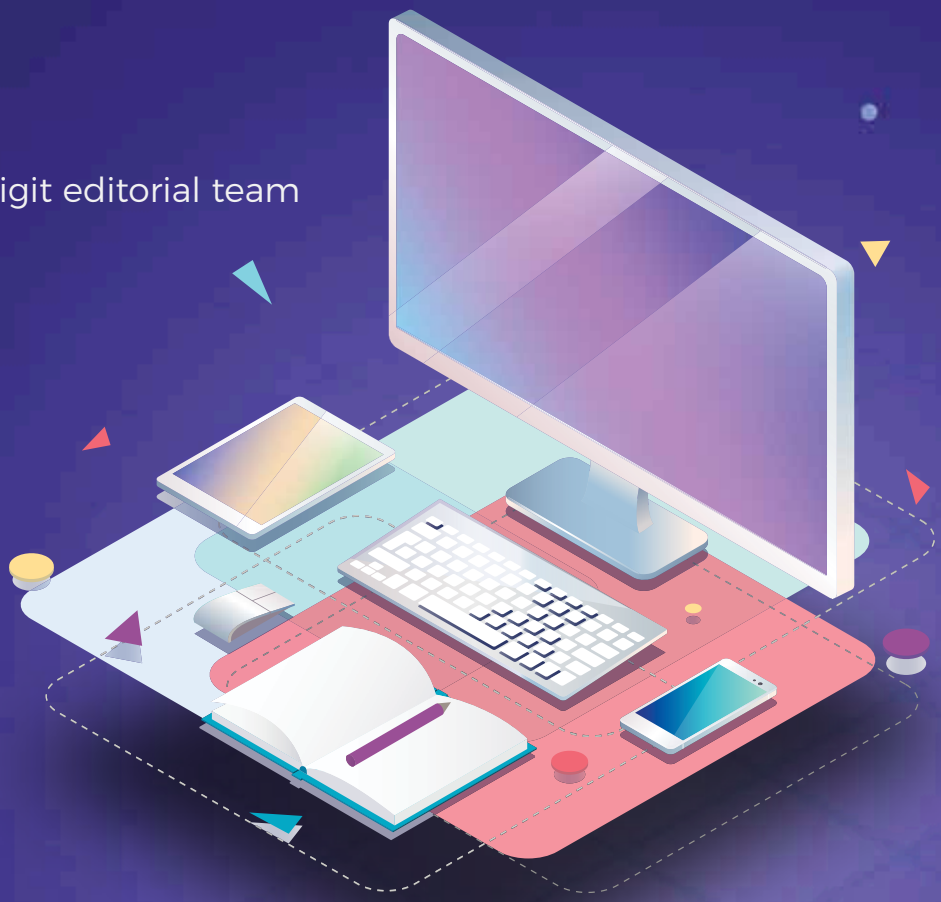
LAUNCHING

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

2021: An Enterprise IT Odyssey

The past was both painful and vexatious. The future promises something bright. But there are still uncertainties on the way

Shyamanuja Das

After last year's extraordinary times, this year comes to us with a lot of hope. For the last six months, we have been talking about the New Normal. Of course, there is a lot of debate around what this New Normal will be – for a company, an industry and the world of business in general.

There are some broad agreements. At least, the discourse has found some common grounds. We will not get into those here. All of you are only too familiar with them.

You also probably know that the elusive New Normal is already upon us—and unveiling a little more of it every day. Rather than trying to get a perfect definition, you would rather try to adjust.

A perfect use case for agile approach in planning!

All we have done in this issue's cover story is try figuring out some of these adjustments, as we have observed by talking to you.

They are not based on any research; so, we do not even claim that these are the most common adjustments. But since this is done basis qualitative inputs from more than 60 CIOs in our various freewheeling interactions, I can surely vouch for their relevance, not comprehensiveness.

In fact, I will be happy if you tell us more. Not just more such adjustments, but even more such situations that require IT to readjust, will be immensely helpful.

There are seven such examples given. The eighth one is a sort of wild card – the acknowledgement that beyond the horizontal trends, businesses have seen strategic shifts in customer behavior, shifts in market dynamics and the ability to offer newer products and services. It will be very difficult for us to try gauging those changes.

I would also like to clarify why I call it an Odyssey, and not just a journey. The past was both painful and vexatious. The future promises something bright. But there are still uncertainties on the way. As Merriam-Websters defines Odyssey, it is "a long wandering or voyage usually marked by many changes of fortune."

But as the same dictionary says, it could also be "an intellectual or spiritual wandering or quest" for all of you.

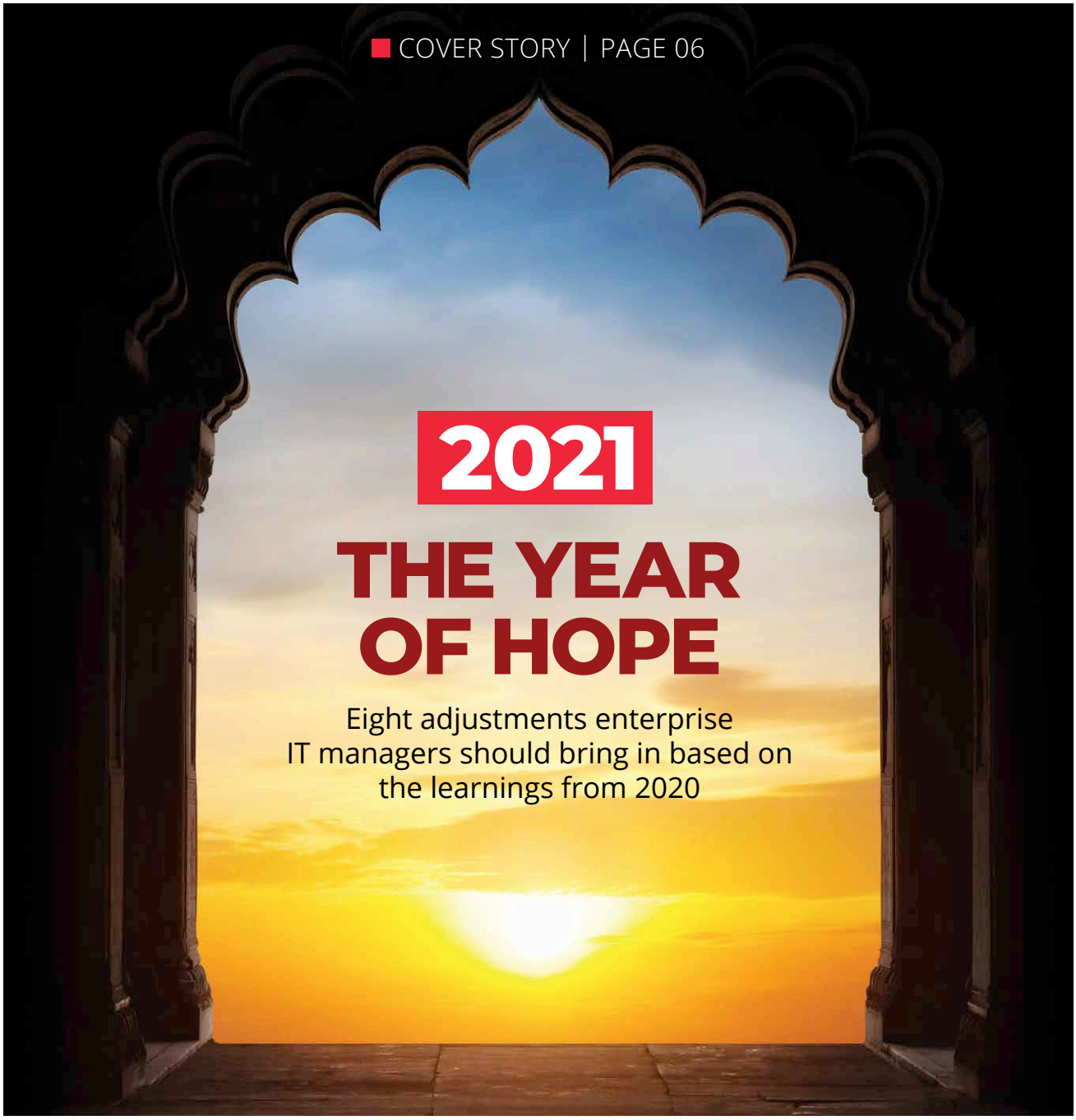
Happy New Year!

Hope we will meet in 2021, physically too. ■

JANUARY 2021
VOLUME 11 | ISSUE 10

Content

COVER STORY | PAGE 06



2021
THE YEAR OF HOPE

Eight adjustments enterprise IT managers should bring in based on the learnings from 2020

Cover Design:
ANIL VK

ADVERTISER INDEX

Bry Air Asia	BC

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

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

EDITORIAL
Editorial Director: Shyamanuja Das
Assistant Manager - Content: Dipanjan Mitra

DESIGN
Sr. Art Directors: Anil VK, Shokeen Saifi
Associate Art Director: Shri Hari Tiwari
Sr. Visualiser: Baiju NV

SALES & MARKETING
Executive Director - B2B Tech:
Sachin Nandkishor Mhashilkar (+91 99203 48755)
Associate Publisher & Director - Community:
Mahantesh Godi (+91 98804 36623)
Associate Director - Enterprise Technology:
Vandana Chauhan (+91 99589 84581)
Head - Community Engagement:
Vivek Pandey (+91 9871498703)
Head - Community - NEXT100 & CIOs:
Megha Bhardwaj
Community Manager - B2B Tech: Renuka Deopa
Senior Manager - Community Development:
Neelam Adhangale

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
Head - Digital & Event Operations: 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

Beefing Up!

NEXT100 Winner 2016 **Bharat Panwar,** DGM/CDT - DS&G/CO, BHEL shares his immense passion for sports besides his love for non-veg food!

"Be Happy, Enjoy Life" is the basic principle I follow in life.
So, going by this principle, I mainly pursue 2 things rigorously:
1. Sports 2. Eating (non-veg)

I believe the above two go hand-in-hand as you have to be fit and play sports. At the same time, eating the right food is also important. People think eating non-veg food is unhealthy and makes you fat. But I believe if you enjoy life and you love something, just go for it. Eating non-veg food in a controlled manner aided with active sports is perfectly alright. What you believe is right, just do it!

A devoted sportsman who never skips his daily game session and a gourmand who loves his meat!

Right since childhood, I've been an avid sports enthusiast and a ferocious non-vegetarian. Cricket has always been my favorite sport besides lawn tennis and table tennis.

I have always been a 'morning' person and irrespective of holidays, my day starts at 5 am. I'm a regular at Siri Fort Sports Complex, where I spend time exercising and playing from 5:30 am to 7:45 am every day. This regular routine helps me to stay fit, healthy and happy. The morning routine rejuvenates me for the entire day. I would recommend all my IT friends to join some sport/physical activity based upon their liking to refresh and enjoy life.

I've participated and led the college cricket team during my engineering days. I've also represented my current organization, BHEL, at national level, namely All India Public Sector Cricket Tournament.

Although nowadays due to time constraint, cricketing activity has reduced, yet I'm ensuring I'm at least involved in active sports beyond cricket, that is in lawn tennis and table tennis. After all, 'once a sportsperson will always be a sportsperson!'

Now, many would agree/disagree with me on this: sports and eating non-veg. But as I mentioned earlier, it is absolutely fine if you can enjoy both by having the right balance between the two. I enjoy non-vegetarian food with my family and friends. My friends and I plan to have it once a week and then relish it to the fullest, even trying out new delicacies. Sadly, this quality time is getting lost with excessive use of social media.

Here, I would like to thank NEXT100 for creating an opportunity to interact and enjoy with a new set of friends. I'm pursuing both my passions now with my NEXT100 friends too. So, hats-off to NEXT100! ■

As told to Dipanjan Mitra, Team ITNEXT

Bharat Panwar

Snapshot

Bharat Panwar is DGM/CDT - DS&G/CO at BHEL. He was a NEXT100 winner in 2016. Panwar has worked in BHEL for more than two decades, right from the beginning of his career. He completed his BTech in Computer Science & Engineering from Himachal Pradesh University.

From music to yoga, a rich repertoire of extra-curricular activities to keep one going

An Extracurricular Mix

NEXT100 Winner 2016 **Mallikarjuna Sarma,** Head of IT - Consultant, Jubilant MotorWorks, CDO, Electrono Solutions and Founder & CEO, SKY Technosolutions shares his variety of extracurricular activities

We all go through so many ups and downs in life and our extracurricular activities keep us rejuvenated. It helps me stay relaxed during my studies, work and other difficult situations.

During my primary education, due to the transferrable job of my father, it was a huge pressure on me to learn different languages in various states without even knowing basic alphabets, but somehow I managed to learn. It was like learning Chinese or Arabic language all of a sudden without knowing the script. I then developed an inclination towards music, dance, spiritual activities and sports. My teachers aided me a lot in these areas.

I started singing Kirtans, Bhajans, Slokas in my primary school and later filmi tunes of Kishore Kumar, SPB, PBS in Telugu, Kannada, Hindi, and Tamil. I was very interested in learning Carnatic, but couldn't get an opportunity when I was younger. I later performed in a few dramas, and film dance was one of my favorites that I learnt and performed on stage in XII and in my engineering college, which was a hit during those days and well appreciated. I also participated in many cultural occasions in my office, singing karaoke, participating in group dance & choreographing a few for my friends. This gave me lot of confidence and satisfaction, and social diversion from my busy software development days.

Later, after a long gap, I found a teacher and learnt Tabla when I was 26 and learnt Carnatic music for over a year when I was 32. My wife, Sowndharya, who is a Chartered Accountant by profession, is also an expert in Carnatic music. She plays the Veena too and is also good at painting.

Sports is something which has always interested me as I used to play Cricket, Shuttle Badminton, Chess and Table Tennis. I won quite a few awards in these sports both in my engineering days and even in office tournaments.

I was inclined towards Indian Vedic studies and always thought to decrypt the inner meaning of scriptures. My Guru taught me some Vedic knowledge like Rudram, Chamakam, Purushasooktam, and Srisooktham.

I have also been connected with spiritual Yoga & Meditation since my childhood. The best Yoga sessions I attended was from Vivekananda Yogic University. I also gained a lot from Isha Yoga videos and various Yoga courses which I undertook. Yoga helped me to relax mentally and re-energize myself. It helped me immensely both personally and professionally.

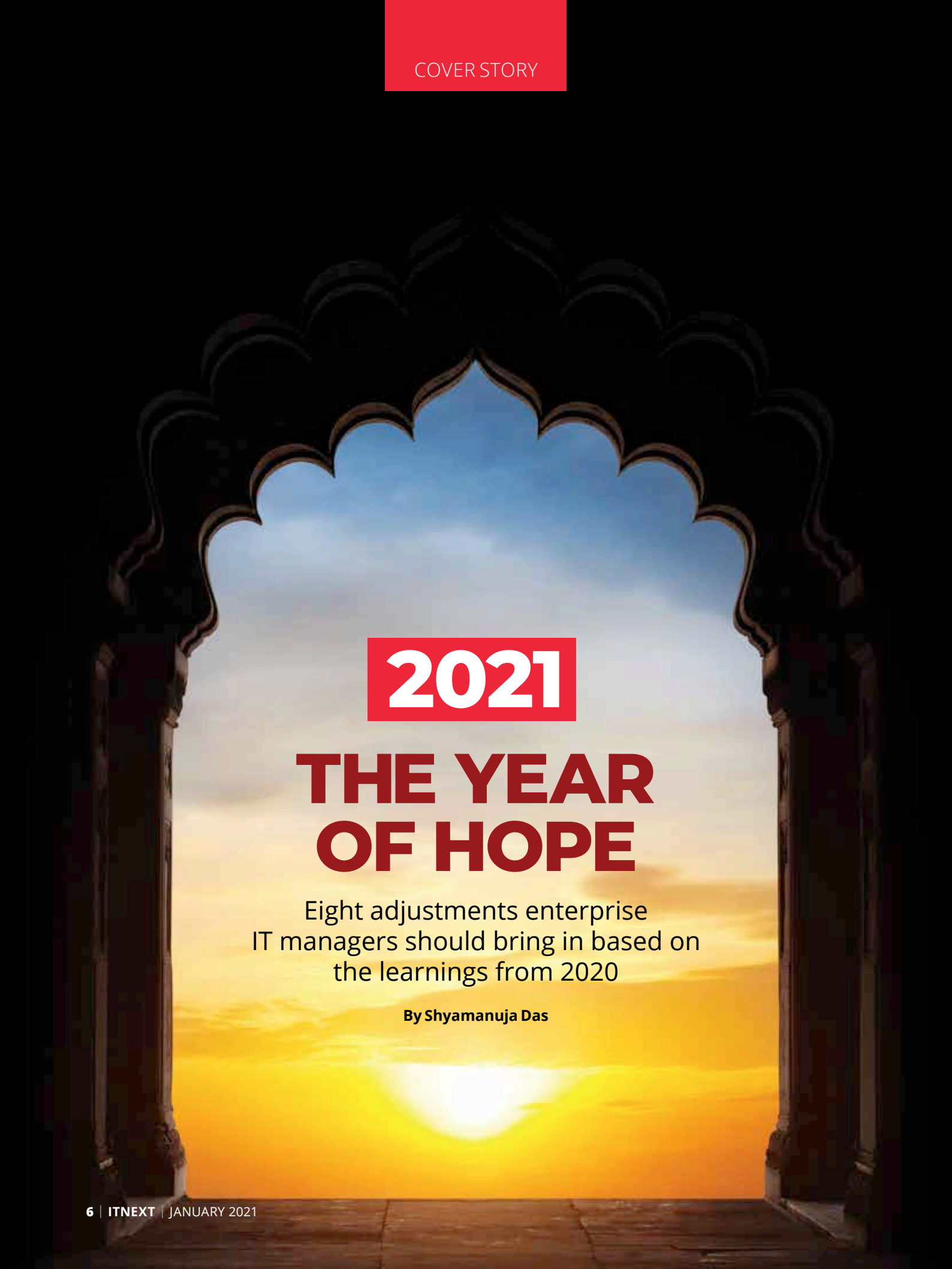
Even now, despite busy work schedule, I try my best to pursue these extracurricular activities to keep me up and running! ■

As told to Dipanjan Mitra, Team ITNEXT

Mallikarjuna Sarma

Snapshot

Mallikarjuna Sarma is Head of IT - Consultant, Jubilant MotorWorks, CDO, Electrono Solutions and Founder & CEO, SKY Technosolutions. He has been a NEXT100 winner in 2016. Sarma completed his MS in Software Engineering from BITS-Pilani and BE in Mechanical Engineering from University of Mysore.



2021

THE YEAR OF HOPE

Eight adjustments enterprise IT managers should bring in based on the learnings from 2020

By Shyamanuja Das

"Tomorrow hopes we have learned something from yesterday," said popular American actor of yesteryears, John Wayne. We have no option but to make our tomorrow hopeful. Never have we—in our lifetimes—seen such a short period teaching us so much, as we have seen in the pandemic-stricken 2020.

It is for us to make sense of the change.

Some changes were just accelerated. We were aware of those changes before COVID but were either not fully convinced or cautious; or were simply procrastinating. COVID just made our decisions easier by leaving us with no option. Digitization of business processes—which itself has so many manifestations—was one such example. It helped the proactive. It convinced the skeptical.

Some changes were absolutely necessary for the situation but may not remain in the long run. They had to be brought in somehow, but as things became more and more normal, companies decided to go back to the older practice. Of course, there were learnings. But by and large, there was a longing to go back to the older practice. Due diligence on security is the most glaring example of a practice that changed during the crisis—no matter what companies claim officially. But they are going back to a tougher stance on security—albeit with newer ways, newer tools to manage.

Some changes were unanticipated but now promise to stay. They came, we saw and they kind of conquered us. Remote working—and all that comes with it—is the most important example of this type of change. The concept was not new per se. But many industries never thought they would have any need to work remotely. Manufacturing, Airlines, Hotels, Insurance... all realized they could work remotely. And the whole world has woken up to the possibility of remote work. The economy, said a commentator, was making a shift to a remote work economy. Whether you agree with that or not, at least no one is saying work from home is a euphemism for leave!

Some changes did not come directly from business organizations' immediate

need to respond to the COVID situation, but from the need to address the changes in marketplace—that is the change in customer behavior, due to a change in lifestyle and spending behavior. Most businesses are still trying to figure out the extent of this change.

Whether it is basic changes like contactless payment methods—India, of course, had learnt a lot of that four years back during demonetization—or the change in demand—either way—for some products and services because the way COVID impacted our lives, these changes are not on-your-face but are more strategic shifts. Examples could include how travel services consumption changed on one end of the spectrum to how consumption of online education and entertainment services changed, on the other. There are the not-so-obvious ones like in manufacturing OT where OEMs wake up to the long-standing needs of opening up to address the security concerns raised by IT in automated plants. But that one demands a full story by itself.

A New Normal response plan, hence, must carefully evaluate all these changes—and we are not saying our classification is the most accurate—and the breadth and depth in which they would impact businesses.

This article goes into a few such changes and their impact on enterprise IT. Again, our claim on these observations is only on their relevance to Indian IT managers and not on the comprehensiveness of their coverage.

But before we get into those adjustments, let's recapitulate some of the most visible changes that all of us have noticed.

They are:

- More collaboration
- More flexibility in workplace model
- Greater security risks
- Traditional Disaster Recovery/Business Continuity plans not being of much help
- Cloud adding a huge use case to itself: that of an effective DR solution
- Companies with greater digitization of business processes responding with far more effectiveness
- Gaps in IT models/digitization getting exposed

We will revisit them when we get into the adjustments.

The adjustments...

#1 Closing the digital gaps

Reliability of a digitized business process is only as strong as its weakest digital link. This was badly exposed during the pandemic time. Digitization in many organizations had been done in bits and pieces. Sometimes, it was a knee-jerk reaction to a teething problem. Sometimes, it was in accordance with the comfort level of the process owner. Sometimes—even though many would not admit it—it was because of a smart technology vendor managing to sell the solution it had. Whatever are the reasons, many realized the hard way that despite 70-80% digitization in some business process, things did not move during the lockdown days, because of the gaps.

Take, for example, supply chains in many manufacturing companies. A lot of it was already automated. But in many organizations, approvals were still manual. In such cases, thanks to people not coming to offices, and thanks to the fear of 'contact', small approvals help an entire chain. There are many other examples—in education, hospitality, even the highly tech-savvy banking sector.

Many scrambled to close those gaps overnight. Some succeeded, some did not. In one chemical manufacturer, the CEO himself mandated to identify such gaps and close them on a priority basis. Of course, many started with the low-hanging fruits—processes where the gaps are small. In 2021, we will see IT managers trying to close the gaps in existing automated processes and go end-to-end in the less automated processes. Expect this to be quite ubiquitous in many industries.

#2 Towards fuller and smoother collaboration

While collaboration tools like Zoom, MS Teams, Google Meet or WebEx saved the day by ensuring that the bare minimum happens and the business ran somehow, by making people talk to each other in groups, the gaps were multiple—and glaring. For one, conferencing is not

When the pandemic struck, data centers were operating fine. There was no threat to the data either. Yet, we know what happened. People struggled to have secure and seamless access to enterprise systems from home. **Right from accessing devices to securing enterprise access, everything was a challenge.**

collaboration. Most of these tools did not have the basic features available in traditional desktop video conferencing like a shared whiteboard. Collaboration requires working together, not pausing to give a briefing or just discussing an idea. That requires smooth, secure and seamless access to applications, which was missing. Security concerns were given a slip, in many cases, just to make people work somehow. Last but not least, the experience on the conferencing tools were, often, less than adequate. If that sounds like a lot of gaps, then be it. But let us not forget that COVID made collaboration an everyday phrase in the workplace and senior executives, who had problem in accessing emails, now swear by collaboration.

So, there is no going back. The functionality, security, and overall experience have to be improved. That, it is a clear top priority for the enterprise IT managers is a no-brainer.

#3 Shift towards human-centric business continuity planning

Most large companies had some amount of business continuity planning in place. Some of them had very meticulous planning. But all of that was around protecting data and technology infrastructure.

When the pandemic struck, data centers were operating fine. There was no threat to the data either. Yet, we know what happened. People struggled to have secure and seamless access to enterprise systems from home. Right from accessing devices to securing enterprise access, everything was a challenge. If the access was secure, there was issue of authorization. Patchwork saved the day for many but created vulnerabilities, that could be—and in some cases were—exploited.

That the traditional business continuity and disaster recovery plans were clearly inadequate was realized soon after the pandemic struck and was a point of discussion. As the pandemic prolonged and most had figured out an ad-hoc solution to make the business running, the issue was forgotten.

"It is a very, very important issue but honestly, I am yet to come across any new and tangible approach," said a CIO. While we have listed optimistically it on the agenda items for 2021, the jury is still out on what could be the approach. As we said in the beginning, it is the year of hope!

#4 Uniformizing IT usage experience

COVID also exposed another major gap. After the first few weeks, when employees were allowed to go to office, many companies decided to stick to work from home. Many of them still do.

But a few employees realized that they did not have remote access to system, while some of their colleagues in other department had. So, even though, work wise, there was no major need for them to be in office (as required for some functional workers), they had to go to office, just because their IT system did not allow them to access their system from home. In other words, they had to risk COVID to go to office while their colleagues stayed home. This less than uniform privilege created much heartache among employees.

This happened because the enterprise IT was not planned end-to-end and certainly not keeping in mind the users. Even as the senior managers, not used to tech so well, have become digital converts post pandemic, the backlash from ordinary employees has the potential to derail many new IT initiates.

This artificial digital divide within the organizations must be addressed immediately.

#5 Renewed interest in smart infrastructure and manageability

Almost every infrastructure and system software vendor has introduced smarter boxes and/or software that could provide a single-pane-of-glass view of the infrastructure for easier manageability. The use case has been managing and thus help in securing hybrid cloud/heterogenous infrastructure well. Not every user organization can identify fully with that.

Most organizations had invested in basic functional boxes that could do what it was basically built to do, without that management layer that would help them to be managed remotely. That is because, even today, the price differential between them and the smarter infra is significant.

COVID, by forcing people to work remotely, brought in a strong use case for intelligent infrastructure that can self-rectify and can be managed remotely smoothly.

Of course, we do not expect people to do a hardware refresh, just for this. But they would certainly be sensitized to realize the need for smarter infrastructure in the next refresh.

#6 More from cloud – catalyzing application modernization

While most large organizations had their tryst with cloud in some form or the other, the pandemic made them realize the value far more than any ROI calculations earlier would have given. As if a new use case of cloud as a business continuity enabler emerged overnight!

Yet not everything was hunky-dory. There were challenges of access, of gaps, and of course, of management and security. And most of those challenges were not because of some inherent problems in public cloud offerings. They were due to the way they were set up.

Cloud made it to most enterprises' hot investment agenda, initially because of the financial advantages that the CFO saw in it—and the conveniences that the CIO saw in it. Those were the low hanging fruits.

As many organizations realized the full potential of the cloud and moved up the value chain, many others were stuck there. For the CIOs, it was not as easy to justify application modernization to the CFO, as it was for infrastructure migration. The comparison was far more tangible and understandable to a finance person for infra migration. So, many applications were migrated in a lift-and-shift manner, the limitations of which were exposed during the extraordinary situation in COVID time.

This, and the new-found acceptance of technology among the conservative corporate honchos, means that we may see application modernization happen faster this year. Though these are often significant decisions, we believe application modernization will actually take off in a big way, thanks to the ecosystem readiness, unlike in case of some of the other adjustments we have talked about.

#7 IT optimization for decentralized operations

One of the clear visible changes brought about by the pandemic is the confidence on remote working. This confidence, coupled with the new reach achieved by many businesses such as education through online, is prompting them to seek a middle path – decentralized workplace, smaller offices in newer locations and hybrid (online + offline) delivery of services.

All these are leading to distributed operations with either mesh or hub-and-spoke model—or a combination of the two. In short, it means the ability to not just establish newer small offices, almost on demand, but to ensure that they are managed centrally with seamless and standardized experience for customers, employees and partners.

In 2021, needless to say, that would essentially be achieved by leveraging technology. It could mean various things. First and foremost, more and more usage of cloud. Second, with local internet access becoming better, thanks to the fiber con-

nectivity becoming widely available even in smaller locations, means, allowing the smaller offices to connect to cloud using local Internet. This, though convenient and cost-effective, has its challenges. That brings us to security and SD-WAN kind of connectivity. Finally, it is the need for manageability, not just that of IT infrastructure but of overall operations, using technology. All these are very real needs and are not rocket science (unlike say reinventing a new DR/BC model, as discussed above). We expect this to happen in a major way this year.

While this is the reactive part, if the experiment works out, businesses would like to make it proactive, by creating a model that would enable plug-and-play enablement of smaller offices.

#8 Readjustment based on strategic business shifts

Apart from the horizontal changes like usage of cloud, shifting to decentralization, more collaboration and better digital processes, which are changes across industries, different businesses have strategic needs based on the market shifts. Many of those needs will have to be fulfilled by leveraging technology. That will, of course, vary from industry to industry but may have lessons for others too.

And now for some wishful thinking: more holistic UX

While technology has removed many a barrier like distance and the limitation of memory and hence has made many things possible, thought to be impossible earlier, it is nowhere close to perfect when it comes to social interactions. That was not really a need in corporate life, as it was taken for granted in an office environment. The pandemic forced us to work in isolation and even showed us many tangible, measurable short-term benefits of remote work, raising the expectations from it.

But the more we work remotely and digitally, the more will machines come in the way of our interacting with each other, noticeability of which will have to be minimized. That would require a different approach to User Experience (UX). UX has traditionally been fairly narrowly defined and has been reduced to a very limited set of metrics. The UX for the New Normal has to be much broader. Some organizations, for example, have introduced a virtual commuting time, for people working from home. This is based on findings that the commuting time acts as a buffer between home environment and office environment and helps the worker switch off gradually from home environment to office environment.

The more we work remotely and digitally, the more will machines come in the way of our interacting with each other... **That would require a different approach to User Experience (UX)**

It is not just about redefining UX. By some of the traditional measures of digital user experience, such as low latency, intuitive interfaces, etc., many IT setups still have a long way to go. Those should ideally be taken up this year.

Endnote

We are yet to comprehend the long-term changes that may take place because of the learnings from the extraordinary situation we faced last year. Of course, every business change will have implications for technology strategies and for CIOs.

While we have identified some adjustments based on what we have observed, it will be presumptuous on our part to call it a definite or a comprehensive list.

But if we do observe something new, we will share with you, right here. ■

NEXTCSO 2020 AWARDS

Meet our winners and jury of 2020...

By ITNEXT

The fourth NextCSO awards were announced digitally on 18th December 2020. This is the first instance of the awards being announced digitally.

The NEXTCSO process started in June 2020—at the peak of lockdown due to the pandemic with self-nomination and filling out a detailed online form.

After completing the application, all candidates had to take two psychometric tests—the Personality Profile Test and the Emotional Quotient test. Both these tests are administered by Central Test of France. As a part of the application process, applicants had to nominate two referees and a supervisor to provide feedback.

Like earlier years, we had a panel of 12 senior CISOs constituting the awards jury. The jury helps formulate the applicant selection criteria—and conducts the interviews.

Using an evaluation model developed in consultation with the jury, we created a list of candidates for interviews. The evaluation model takes into account candidates' academic achievements, the length and quality of work experience, certifications, and the psychometric test scores.

Each selected candidate was interviewed by two jury members independently. To get selected for the award, a candidate had to be approved by both the jury members.

That only 18 could make it to the list of winners from the 851 who applied is a testimony to the level of competition that one has to go through before they emerge winners.

We present here those 18 successful candidates—India's future CISOs. They join the winners of NextCSO of the first three batches—in 2015, 2017 and 2018—in this exclusive club.


nextCSO
AWARD
2020
CSOFORUM

INDIA'S FUTURE SECURITY LEADERS

nextCSO WINNERS 2020

Indranil Chatterjee
General Manager – Security & Compliance, Jio Platforms

Hemant Chavan
Head – Information Security, TietoEVRY

Kishor Gojiya
Head – IT, CIMS Hospital

Smita Jain
Cyber Security Technology Specialist, Microsoft India

John Joseph
Cyber Security Officer, Calyx

Mukund KS
General Manager – IT, Inventia Healthcare

INDIA'S FUTURE SECURITY LEADERS

nextCSO WINNERS 2020

Mukesh Kumar
Vice President & Head – Enterprise IT Infrastructure, Mphasis

Vijay Mishra
Director & IT Business Partner, Capgemini

Vasanth Pai
Assistant Vice President, Tech Mahindra

Syed Raheem
IM Security Head, Amara Raja Group

Vikram Raj
Assistant Vice President, Barclays

Kunal Rangole
Associate VIce President – Information Security & BCM, Evalueserve

INDIA'S FUTURE SECURITY LEADERS

nextCSO WINNERS 2020

Prakash Kumar Ranjan
Senior Manager, Airtel Payments Bank

Jagannath Sahoo
Head – Service Delivery, Bharti Airtel

Ambarish Kumar Singh
Senior Manager, Flipkart Internet

Nikesh Sinha
Principal Consultant, Hinduja Global Solutions

Sandeep Solanki
Assistant General Manager, Secure Meters

Sangameshwar Yallawaram
Associate Vice President, Broadridge Financial Solutions (India)

INDIA'S FUTURE SECURITY LEADERS

nextCSO JURY 2020

Makesh Chandramohan
CISO, Aditya Birla Financial Services Group

Uday Deshpande
CISO, Larsen & Toubro Group

Durga Prasad Dube
Senior Vice President & Global CISO, Reliance Industries

Sridhar Govardhan
Senior Director & Head – IS, Flipkart Internet

Lucius Lobo
CISO, Tech Mahindra

Murli Menon
CSO – GDC India & Atos India, Atos Global IT Solutions and Services

Dr Rudra Murthy
CISO, Amazon Pay

Aashish Narkar
Global Head – IT Security (Internal IS) & CISO, Tata Consultancy Services

Manoj Nayak
CISO, SBI Life Insurance

Yask Sharma
CISO, Indian Oil

Vinit Sinha
Director – Cybersecurity, Mastercard

Anuj Tewari
CISO, HCL Technologies

Spreading Attacks From Space – Cybersecurity Threat Predictions For 2021

Going into 2021 and beyond, we face a significant shift in the cyberthreat landscape with the rise of new intelligent edges, which is about more than just end-users and devices remotely connecting to the network

By Rajesh Maurya

In 2020, we saw many rapid changes on a global scale as organizations across the world attempted to adapt to a New Normal caused by the pandemic. Amid this shift, there were significant developments seen across the cyberthreat landscape. Going into 2021 and beyond, we face another significant shift with the rise of new intelligent edges, which is about more than just end-users and devices remotely connecting to the network.

In FortiGuard Labs' threat predictions for 2021, we've estimated the strategies that we anticipate cybercriminals will leverage in the coming year and beyond. This includes, but is not limited to, predictions and insights on intelligent edge computing, 5G-enabled devices, and advances in computing power, as well as the new wave of advanced threats that will undoubtedly arise as a result.

Each year at this time, we take a look at trends across the cyberthreat landscape, whether just around the corner or further afield. Predicting security threat trends may seem like more art than science, but the reality is that combining a strong understanding of how threats develop and what sorts of technologies cybercriminals gravitate towards both to use and to exploit with evolving business trends and strategies helps make predictions a reasonable process.

The Intelligent Edge is a Target

Over the past few years, the traditional network perimeter has been replaced with multiple edge environments, WAN, multi-cloud, data center, remote worker, IoT, and more, each with its unique risks. One of the most significant advantages to cybercriminals in all of this is that while all of these edges are interconnected many organizations have sacrificed centralized visibility and unified control in favour of performance and digital transformation. As a result, cyber adversaries are looking to evolve their attacks by targeting these environments and will look to harness the speed and scale possibilities 5G will enable.

Corporate network attacks launched from a remote worker's home network, especially when usage trends are clearly understood, can be carefully coordinated so they do not raise suspicions

Trojans Evolve to Target the Edge

While end-users and their home resources are already targets for cybercriminals, sophisticated attackers will use these as a springboard into other things going forward. Corporate network attacks launched from a remote worker's home network, especially when usage trends are clearly understood, can be carefully coordinated so they do not raise suspicions. Eventually, advanced malware could also discover even more valuable data and trends using new EATs (Edge Access Trojans) and perform invasive activities such as intercept requests off the local network to compromise additional systems or inject additional attack commands.

5G Can Enable Advanced Swarm-Attacks

Compromising and leveraging new 5G-enabled devices will open up opportunities for more advanced threats. There is progress being made by cybercriminals toward developing and deploying swarm-based attacks. These attacks leverage hijacked devices divided into subgroups, each with specialized skills. They target networks or devices as an integrated system and share intelligence in real time to refine their attack as it is happening. Swarm technologies require large amounts of processing power to enable individual swarm-bots and to efficiently share information in a bot swarm. This enables them to rapidly discover, share, and correlate vulnerabilities, and then shift their attack methods to better exploit what they discover.

Advancements in Social Engineering Attacks

Smart devices or other home-based systems that interact with users, will no longer simply be targets for attacks, but will also be conduits for deeper attacks. Leveraging important contextual information about users including daily routines, habits, or financial information could make social engineering-based attacks more successful. Smarter attacks could lead to much more than turning off security systems, disabling cameras, or hijacking smart appliances, it could enable the ransoming and extortion of additional data or stealth credential attacks.

New Ways to Leverage Ransomware in Critical Infrastructures

Ransomware continues to evolve, and as IT systems increasingly converge with operational technology (OT) systems, particularly critical infrastructure, there will be even more data, devices, and unfortunately, lives at risk. Extortion, defamation, and defacement are all tools of the ransomware trade already. Going forward, human lives will be at risk when field devices and sensors at the OT edge, which include critical infrastructures, increasingly become targets of cybercriminals in the field.

Advances in Cryptomining

Eventually, by compromising edge devices for their processing power,

Quantum computing could create a new risk when eventually it is capable of challenging the effectiveness of encryption in the future

cybercriminals would be able to process massive amounts of data and learn more about how and when edge devices are used. It could also enable cryptomining to be more effective. Infected PCs being hijacked for their compute resources are often identified since CPU usage directly impacts the end-user's workstation experience. Compromising secondary devices could be much less noticeable.

Spreading Attacks from Space

The connectivity of satellite systems and overall telecommunications could be an attractive target for cybercriminals. As new communication systems scale and begin to rely more on a network of satellite-based systems, cybercriminals could target this convergence and follow in pursuit. As a result, compromising satellite base stations and then spreading that malware through satellite-based networks could give attackers the ability to potentially target millions of connected users at scale or inflict DDoS attacks that could impede vital communications.

The Quantum Computing Threat

From a cybersecurity perspective, quantum computing could create a new risk when eventually it is capable of challenging the effectiveness of encryption in the future. The enormous compute power of quantum computers could render some asymmetric encryption algorithms solvable. Although the average cybercriminal does not have access to quantum computers, some nation-states will, therefore the eventual threat will be realized if preparations are not made now to counter it by adopting crypto agility.

Artificial Intelligence (AI) Will Be Key

As these forward-looking attack trends gradually become reality, it will only be a matter of time before enabling resources are commoditized and available as a darknet service or as part of open-source toolkits. Therefore, it will take a careful combination of technology, people, training, and partnerships to secure against these types of attacks coming from cyber adversaries in the future.

AI Technology Needs to Keep Up

The evolution of AI is critical for future defense against evolving attacks. AI will need to evolve to the next generation. This will include leveraging local learning nodes powered by ML as part of an integrated system similar to the human nervous system. AI-enhanced technologies that can see, anticipate, and counter attacks will need to become reality in the future because cyberattacks of the future will occur in microseconds. The primary role of humans will be to ensure that security systems have been fed enough intelligence to not only actively counter attacks but actually anticipate attacks so that they can be avoided.

Organizations Can't Do It Alone

Organizations cannot be expected to defend against cyber adversaries on their own. They will need to know who to inform in the case of an attack so that the "fingerprints" can be properly shared and law enforcement can do its work. Cybersecurity vendors, threat research organizations, and other industry groups need to partner with each other for information sharing, but also with law enforcement to help dismantle adversarial infrastructures to prevent future attacks. Cybercriminals face no borders online, so the fight against cybercrime needs to go beyond borders as well. Only by working together will we turn the tide against cybercriminals. ■

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

Application Security In A Multi-Cloud World

As applications migrate to the cloud, gaining actionable visibility into application health and service-level agreements (SLAs) becomes critical since each application may require a different tool to monitor performance

By Nikhil Taneja

Management of applications in heterogeneous cloud environments introduces new challenges for IT, DevOps and application owners. One of the challenges of this is that each environment offers different capabilities, resulting in inconsistent management and deployment of application delivery and security services, policies and configurations.

As applications migrate to the cloud, gaining actionable visibility into application health and service-level agreements (SLAs) becomes critical since each application may require a different tool to monitor performance.

In such a dynamic environment where each application has its own set of requirements, it is almost impossible to accurately plan for the application delivery and security licenses required for each environment. As a result, IT departments face risks when budgeting for application delivery and security solutions.

Microservice & Security

As organizations transition to the

cloud, many are adopting microservice architecture to implement business applications as a collection of loosely coupled services. Some of the reasons to move to this architecture are to enable isolation, scale, and continuous delivery for complex applications. Many of these loosely coupled services are also Function-as-a-Service (FaaS) and use Representational State Transfer (ReST) APIs.

That's a lot of attack surface which wasn't exposed when the applications were monolithic. Adopting microservices doesn't remove the traditional security and application availability concerns. Hackers are also taking advantage of internet turning dark – increasing adoption of SSL encrypted traffic.

Most Successful Attacks

The recent ransomware attacks highlight the need to secure against denial of service and application attacks.

That's a lot of attack surface which wasn't exposed when the applications were monolithic. Adopting microservices doesn't remove the traditional security and application availability concerns. Hackers are also taking advantage of internet turning dark – increasing adoption of SSL encrypted traffic.

Attacks are More Successful

The recent ransomware attacks highlight the need to secure against denial of service and application attacks. The primary goal of cyber-attacks is service disruption, followed by data theft. Service disruption creates poor customer experience, and perpetrators know that and use a broad set of techniques to cause harm. These include bursts of high traffic volumes, which do not leave time for mitigation teams to get a grip, usage of encrypted traffic to overwhelm security solutions resource consumption, and crypto jacking that reduces the productivity of servers and endpoints by enslaving their CPUs for the sake of mining cryptocurrencies.

The recent ransomware attacks highlight the need to secure against denial of service and application attacks. The primary goal of cyber-attacks is service disruption, followed by data theft. Service disruption creates poor customer experience...

The primary goal of cyber-attacks is service disruption, followed by data theft. Service disruption creates poor customer experience, and perpetrators know that and use a broad set of techniques to cause harm. These include bursts of high traffic volumes, which do not leave time for mitigation teams to get a grip, usage of encrypted traffic to overwhelm security solutions resource consumption, and crypto jacking that reduces the productivity of servers and endpoints by enslaving their CPUs for the sake of mining cryptocurrencies.

Attacks are also more targeted and more successful – more result in a complete outage rather than merely service degradation. According to Radware research, data breaches are expensive, and the costs are only going up. Those reporting attacks that cost 10 million USD/EUR/GBP or more almost doubled last year — from 7% in 2018 to 13% in 2019. Half of the respondents estimated that an attack cost somewhere between 500,001 and 9.9 million USD/EUR/GBP.

Every cloud has a different option, product offering and ways of securing applications. This is one critical area where you MUST standardize profiles and policies for your applications. Application protection is a lot more than just preventing OWASP Top 10 attacks. In addition to protecting applications against XSS, SQL Injection, and others it is also about protecting against API abuse, bad bots, vulnerability exploits and application denial of service.

Best Practices

Secure application delivery best practices include:

- Applying consistent policies across multiple deployments
- Preventing configuration errors from creeping in during deployment by automating as much as possible
- Addressing issues such as phishing and social engineering that play a large part in human failures
- Ensuring that the applications are accessed by the right users that are authorized and authentic
- Keeping all attacks out of the corporate / virtual private networks
- Gaining actionable visibility

As many of us are now working remotely, organizations have moved many of their applications to the cloud to take advantage of the flexibility. This does address the immediate need to scale access but creates many security challenges that must be addressed to keep both customer data and corporate IP and businesses safe from hacking attempts. Part of the solution is to address the human aspects of security weakness by educating and automating, the other aspects are to adopt best practices and implement multi-layered approach to securing these applications. ■

The author is Vice President & Managing Director - India, SAARC, Middle East & GSI at Radware

The Automation Journey – A Practical Roadmap To Success

Automation is a smart investment for companies seeking to elevate their service delivery and customer experience

By Anuj Vaid

Automation is a smart investment for companies seeking to elevate their service delivery and customer experience.

No matter how well-oiled your delivery engine, there is a chance for errors; especially when it involves time-consuming, complex and repetitive tasks. Your automation journey begins here - with the errors that cause customer delay and aggravation. These gaps are your optimization and automation opportunities.

Once you've identified the processes that can be optimized, you can use digital tools to automate the tasks and workflows. This will reduce errors, complexity and wait-time, making your operations run smoothly and efficiently.

For example, your customers might have questions about your product or need help in installing a new version of software. They might need this information/support urgently, maybe outside office hours. Or they might find the long wait-time for phone support frustrating. To support them, offer an omni-channel chatbot service that answers questions and guides them through the installation in real time. With this innovative swap, you empower your customers to access support 24/7 without expending additional resources.

For one of the largest telecom companies in India, we've developed a chatbot-powered IT Service Desk that has become the first line of resolution for over 20,000 users. In the last year, over 80,000 conversations led to the resolution of 100,000 queries, with an amazingly meagre 0.5% call abandonment rate. And, the service desk ticket volume dropped by a staggering 74%.

What can be automated?

At the heart of automation is innovation. Automation has innumerable use cases—from complex scenarios like compliance to routine tasks like password resets. Any business process that follows a rule can be automated. Daily checklist tasks that are monotonous and time consuming are ideal automation candidates.

Let's return to our chatbot example. It is a programme that simulates human conversation. Your customers ask questions using a text chat box or voice command. The software analyses the words and returns predefined answers. After an initial setup (list the frequently asked questions and feed in the appropriate answers), it learns on the go and becomes smarter with minimal human intervention.

Traditionally, companies expend a lot of resources in helping their customers use their products or services. A single fixed cost investment in setting up a chatbot, with minimal further investment in updating and maintaining it can replace this expense easily. The result? Savings of time, money and human ingenuity that can be leveraged to take the enterprise to the next level.

Any business process that follows a rule can be automated. Daily checklist tasks that are monotonous and time consuming are ideal candidates

Even the administration of customer service can be automated. Tickets can be auto-created, allocated and closed. Many problems, such as password reset, access requests and resetting VPN/network configurations can be taken care of through self-help and self-heal solutions.

Multiple chatbots can run multiple processes, often interconnected with each other, with underlying systems such as ERP, HRMS, etc. and can be commissioned quickly using our cloud-based chatbot platform. Each bot can also be integrated with a 'Live Agent' to ensure that there are no unsatisfied customer drop-off's.

If innovation is the goal of a company, automating the helpdesk is the prime innovation that enables all others. The best part is that you can outsource the chatbot and its related activities to a Managed Service Provider (MSP). Your MSP will deploy and run the service for you.

We've helped a major pharmaceutical company efficiently manage its user requests with zero drops thanks to help-desk automation services augmented with a chatbot/conversational AI. This solution led to 24/7 availability with lean resources, 90% error reductions, and a whopping 50% increase in first call resolution.

Frequent areas of chatbot use are: Customer Service, Help Desk, Guided-Self Service, HR, Solution Navigation, and MIS Reporting. These are some common IT tasks that are prime candidates for automation:

- Creating, allocating, and closing support tickets
- Patch management
- Backup and storage management
- NOC services like co-relation of alerts and removing false positives or detecting potential threats and issuing early warnings
- Escalation triggers can be automated with the help of RPA and other tools

Key benefits

- **Increase productivity:** With the same amount of human capital

Automation requires a company to change the way it delivers value. Innovation is driven through automation. It requires openness to change, and the constant desire to do things better. Chatbots learn, so the journey gets better with its intelligence

as before, you can now get more done, as that human capital is freed up to work on non-mechanical tasks.

- **Reduce costs:** Automation mainly consists of a single fixed capital cost. Let alone having to pay salaries and offer raises, automation is likely to get cheaper with time.
- **Boost accuracy/quality:** Humans are prone to making mistakes on repetitive tasks. On the other hand, a script that automates a repetitive process will produce results without any error or oversight.
- **Enhance customer experience:** Being able to receive help 24x7 from discerning, ever-ready chatbots will keep customers satisfied and loyal.
- **Improve analytics:** Each process and interaction yields data. When these are taking place through automation, the data can immediately be yielded and utilized to improve operations through the built in Artificial Intelligence/ Machine Learning capability.
- **Elevate employee experience:** Having the basic, time-consuming tasks automated frees up employees to actualize their full potential. With this, employees find work meaningful and enjoyable. Millennials are looking to do more with less, and such bots create great user experience.

Change management is the key

Automation requires a company to change the way it delivers value. Innovation is driven through automation. It requires openness to change, and the constant desire to do things better. Chatbots learn, so the journey gets better with its growing intelligence. Like with any of us, it needs to be supported through its learning journey. Automation can take over entire tasks and make some roles redundant. That can be daunting. You need to proactively anticipate resistance, overcome this with transparency and help your people to upskill and reskill. Involve the most impacted employees in the change management process and help them adopt new ways of thinking.

Tips for successful automation

- Choose processes wisely, i.e. those that will yield the greatest results. Processes that are repetitive, stable, work with digital data inputs, run on structured data, and don't require human judgement are ideal.
- Appoint change champions to lead, guide and cheerlead the organization through the change. This is essential to unlocking the true value of automation.
- Break silos. Automation works best when you foster collaboration across teams, share data with other functions, and proactively build cross-functional/enterprise-wide workflows and processes.

Deploying automation/conversational Bot's and RPAs is akin to having an intelligent, digital workforce that delivers value 24/7. It's an investment that will pay for itself many times over. ■

The author is EVP, CMS IT Services

Leveraging Salesforce Marketing Automation For Driving Business Success

Marketing teams are leveraging the use of new-age technology – salesforce marketing automation for seamless execution of marketing campaigns

By RS Maan

The present world of business is transforming with the advancements and adoption in technology. Customer journey and the way they interact with a brand has also been transformed like never before. The brands are targeting customers, providing personalized experiences based on their requirements.

The customers are overloaded with marketing messages on different channels. Developing a message tailored to specific customer data is challenging. In such a scenario, brands need to create marketing campaigns that stand out in the market. The marketing teams are utilizing digital chan-

nels to create ideas that are innovative and enticing for the customers. There is no denial of the fact that executing day-to-day marketing campaigns according to the customers' dynamic behavior and preferences involves several challenges.

To focus on the bigger picture, marketing teams are leveraging the use of new-age technology – salesforce marketing automation for seamless execution of marketing campaigns. It automates processes that makes the sales team directly approach prospective customers through a combination of tactics. Before moving forward, it is imperative to understand what 'salesforce marketing automation' is all about?

In today's competitive world of business, every brand has to be omni-directional in the planning and execution of marketing campaigns. Salesforce marketing automation is a technology that automates the management of multiple marketing activities and multifunctional campaigns. It simplifies the targeting of potential customers with automated messages across various digital platforms – email, web, and social. Additionally, it automates the process of sending messages by using custom-built templates.

How does salesforce marketing automation help in business growth?

Salesforce marketing automation is becoming widely popular among sales and marketing departments. Lead generation is one of the topmost priorities for the sales team and it has become an extremely essential step in growing businesses. Automating the important marketing processes and campaigns saves the time of the sales team and lets them focus on the overall strategy of handling leads and enhancing customer experience. The salesforce marketing automation software is designed for business scalability. By using a strategic set of tools, it simplifies the complex and time-consuming responsibilities by effectively handling repetitive tasks and reducing human error.

Automating the important marketing processes and campaigns saves the time of the sales team and lets them focus on strategy

How is salesforce marketing automation valuable?

Salesforce marketing automation is one of the most marketable and profitable platforms for business growth. Companies offering breakthrough services and products need an exhaustive platform for targeting customers. Additionally, the widespread adoption of digital channels makes the cloud-based platform more functional.

Customer Acquisition

Every business needs customers to survive, grow and sustain. In previous times, sales executives used to rely on cold calling and emailing for reaching out to customers. But strong internet presence has transformed the process of lead generation. Salesforce strategically generates leads, qualifies, manages and sends them to the sales team. It uses behavioral details of the customers that help the marketing teams in analyzing their interests and purchase behavior. It brings together information of customers from website visits, downloads, and social media activities to automate lead qualification.

Monitoring progress of marketing campaign

Salesforce marketing automation gathers essential customer data that can be monitored and measured. The proper implementation of marketing automation helps in tracking the progress of the campaign. By identifying critical sales data, it defines KPIs (key performance indicators) that makes the marketing automation process measurable. Furthermore, the dashboard helps in monitoring monthly targets, marketing performance, pipelines to understand the real leads and those under development.

Improves marketing strategy

Marketing automation works beyond automating lead generation process. Based on customer data and behavior, the sales and marketing teams establish clear objectives post understanding the customer's purchase cycle. Additionally, the marketing executives are able to measure the effectiveness of the touchpoints that are set by the teams for customer acquisition. This further allows the brands to analyze their overall campaign performance and efficacy. It further removes the guesswork in deciding the touchpoints and formulating an important business marketing strategy.

Improves marketing ROI

Automating the marketing processes removes manual intervention to plan and send emails and messages. This saves the time of the team and lets them focus on other tasks such as analyzing the important customer data and tweaking marketing plans according to the campaign performance. An automated strategy helps in making the team focus on those factors that drive revenue and improve ROI, alongside growing the business.

The success of the campaigns depends upon personalizing marketing messages for customers. The effective implementation of marketing automation transforms lead generation and nurturing. It comprehensively works in customer acquisition, conversion, and retention that ultimately leads to increased sales and sustained business growth. ■

The author is Global CRO at Codleo Consulting

How BFSI Uses Technology-Driven Culture To Make Their Workforce Future-Ready

Banking and financial services, a critical pillar of the economy, has seen a major shift from the physical and traditional ways of operations. It has accelerated a never seen before digital push and a wider and larger financial ecosystem

By Prasoon Nigam

As the work from home regime for everyone amidst the Coronavirus pandemic, providing customer assistance and services is now becoming the norm. The world has witnessed an inescapable reality in the name of COVID-19 and has turned our outlook upside down on perhaps everything we knew.

The infectiousness of Coronavirus is not a 'normal' one, and has disrupted value chains, communication, and operations like never. For FinTech and BFSI companies, the pandemic has been a real eye opener. It has drastically impacted business continuity and business models. Banking and financial services, a critical pillar of the economy, has seen a major shift from the physical and traditional ways of operations. It has accelerated a never seen before digital push and a wider and larger financial ecosystem.

A global analysis by Accenture stated that 79% of the banking executives agreed that there is an immediate need to re-engineer the experience that brings people and technology together. At the same time, 17% believe that AI is a critical aspect of their orientations. The findings showcase the belief of BFSI executives in the power of digital transformation. Whether be it front end customer services or the last mile, digital solutions have become the foundation stone for FinTech companies to curate customer experiences, retain and grow their market share.

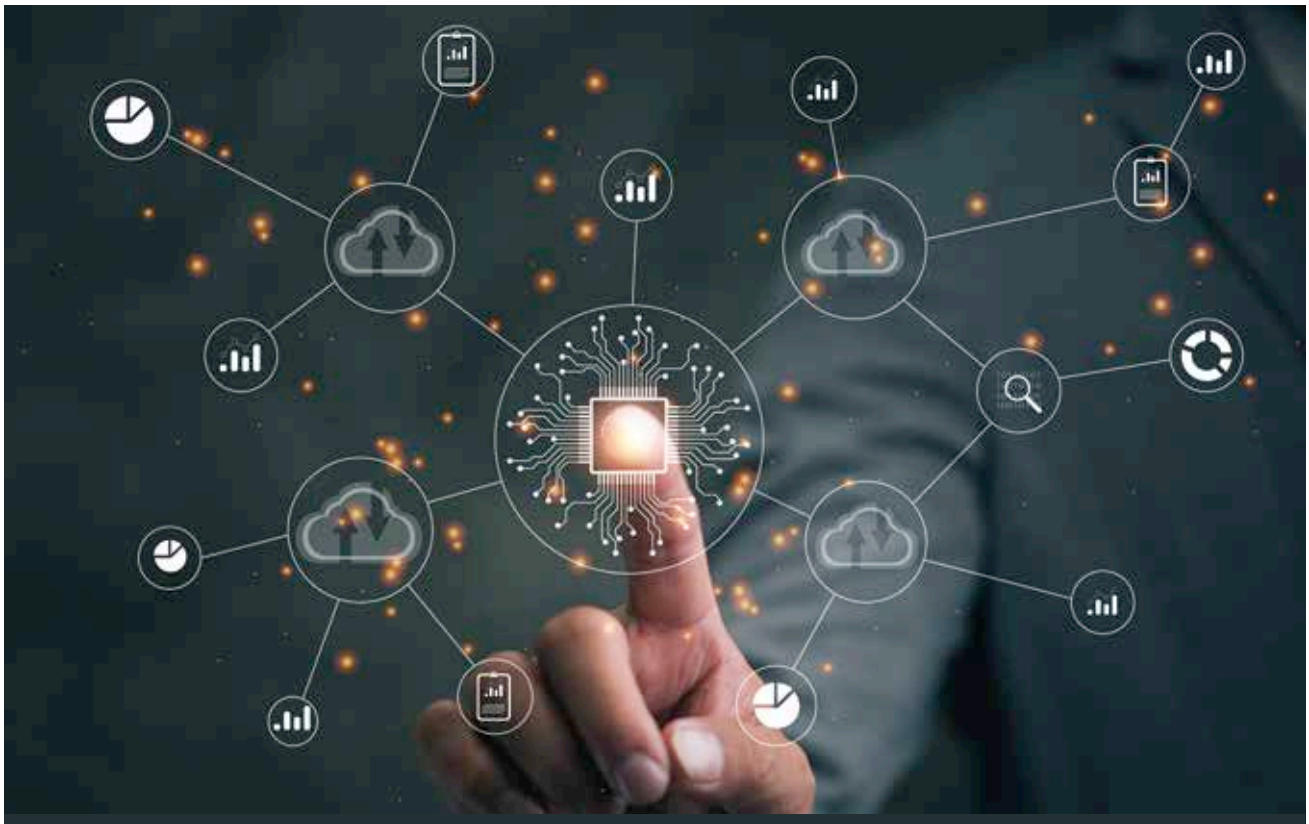
Even before the pandemic, businesses had already implemented these digital and automation strategies for more efficiency of operations. However, as the crisis unfolded, financial institutions have responded quickly to the new scenarios by designing and launching new digital products to make everything accessible in real-time. The new financial ecosystem has seen emergence of new technologies; for interfaces – application programming human computer interface, workflow automation for internal and external functions, hybrid cloud services, AI and data driven storage and management and blockchain among others to streamline operations. Going forward, the sector will see a massive shift from branch banking, as customers get accustomed to digital processes, and would therefore prefer the enhanced convince and speed of operations. Further, many AI and ML-based applications are enabling companies to streamline credit lending, and processing operations, and customer interactions. From higher returns and operational efficiency, to lesser costs, a digital infrastructure will contribute to every arena of the financial value chain.

But simply being more digital or online is not going to cut it. From core banking, lending, insurance, or wealth management – digital now needs to be the backbone...

But simply being more digital or online is not going to cut it. From core banking, lending, insurance, or wealth management – digital now needs to be the backbone to ensure efficiency and efficacy. As BFSI players calibrate for the future, operations become digital and employees collaborate virtually from remote locations, it will also be important to build strong mechanisms in tackling cyber security concerns and risks. In such a scenario, more standardization and connectivity will be needed to unlock the potential of an all-digital ecosystem, which also necessitates more regulations and policies to drive this transition.

The prevalence of a contactless environment and social distancing has certainly steered a clear path to digitization and for the BFSI industry to move away from conventional and traditional. As financial institutions aspire for more agility in the New Normal, there needs to be a deeper review of practices, and controls to upgrade to ensure business continuity. With business no longer as usual or 'Normal', it is time for BFSI 2.0 which thrives on a digital – a futuristic collaborative ecosystem of all services and stakeholders. ■

The author is CTO & Co-Founder, Stratbeans



2021 Predictions: More Power To Digital And Data In The Recovery Phase And Beyond

The IT sector undeniably became the backbone of the all-new digital world and subsequently the pressure on the tech infrastructure became overwhelming, giving rise to the need for a renewed business strategy in 2021

By Ramesh Mamgain

The pandemic brought the world almost to a standstill and making us step back and ponder how we could have done things better! The IT sector undeniably became the backbone of the all-new digital world and subsequently the pressure on the tech infrastructure became overwhelming, giving rise to the need of a renewed business strategy in 2021.

Sustainable Compassionate Leadership

While the IT sector has been at the forefront in aiding the public authorities and enterprises to combat one of the biggest health, economic and human crisis of our times, the pervasiveness of digital has forced companies to crave for sustainable digital transformations. We are already seeing this change, with smarter enter-

prises taking the right steps towards leaving greener footprints.

One good thing that came out of this crisis is that it has brought the entire world together, stressing the need for true leadership driven by resilience and compassion. Adoption of the virtual workplace has indeed boosted productivity, but the real challenge business leaders will face in the coming time will be to ensure the mental and physical wellness of their associates, so as to steer away from the perils of being cocooned. This will be not only vital for creating a healthier work culture but also for retaining talented resources workforces and thrive despite the uncertain times.

Data Driven Digital Transformation

As we step into the post COVID era, digital transformation has become the new norm for companies - big and small. The rise in the distributed workforce, virtual engagements, and a broad array of devices we use to operate, plan and respond to this crisis will continue to generate exponential data.

Business leaders will be seized with the challenge of how to secure such a large volume of fragmented data. This is where federated control of data will be given priority along with data recovery and back up mechanisms, systems and tools, mitigating risk and ensuring business continuity.

This is also where data management experts will come in, empowering organizations with higher security, gaining control of this fragmented data, while unlocking strategic insights to be future ready against the looming threats of ransomware and economic uncertainty.

Inching towards Intelligent Data Protection

The cyber security space has become more complex due to pandemic and will remain so in 2021. Security has lately been at the top of the priority list for CIOs, with the pandemic bringing data protection to the forefronts.

The expansive work from home practices has added to enterprise vulnerabilities which the attackers can easily take advantage of. In 2021, we will continue to see new pervasive ransomware trends, apart from encrypting victim's data, the hackers will also threaten to publish sensitive or confidential information, if their demands are unmet.

In order to thwart the hackers, we will see more enterprises ramping up their data protection, making Intelligent Data Management more sought after by enterprises than ever. As data recovery becomes critical, it will heighten the need for balancing privacy with health and security.

Business leaders will be seized with the challenge of how to secure such a large volume of fragmented data. This is where federated control of data will be a priority

Into the Clouds with Data

One of the biggest trends that the year 2020 saw was the rapid adoption of cloud platform across the board. Migration of cloud has opened creative and sustainable ways to have more control and insight into data, which in turn will enable organizations to leverage on various opportunities, such as modernizing and scaling up of processing and storage capabilities, better management and reduction of costs while encouraging remote collaboration and ensuring data availability through smarter disaster recovery strategies.

India had made rapid strides in its Digital initiatives, from the National Health Digital Mission to the Digital India initiatives, making data all the more important and critical an asset. This new need will demand adept skill sets and professionals to understand the disparate data sets – from structured to unstructured ones. We will see automation and AI tools coming in to help find and secure this data on the go and enterprises will make a deliberate choice of where and how they want their data to be placed.

Hybrid World is the New World

The cloud adoption was just step one in the evolution of the enterprise's journey; the real test will be the sustenance phase. One this is for sure - organizations will move away from conventional infrastructures because the times are evolving and so are their needs.

Bearing cost in mind enterprises will look at the path to drive economies of scale, and the good news is cloud and connectivity of this digital path will give them just that. This does not mean that we will become an all-virtual world. After all, human beings are social animals, hence we will see each organization defining its own unique processes, striking the balance between remote and physical worlds. This will stand true for their business models, operations, and to their cloud choice.

Indeed, we are going through an unprecedented technological revolution with disruption everywhere. As every business becomes a data-driven business, better data governance and data protection driven by progressive leadership and culture will become existential for all enterprises.

The future indeed looks promising and full of opportunities, but are the enterprises 'Ready' to embrace the change and realize their full potential? ■

The author is Country Manager for India & SAARC at Commvault

The Modern Architect: Accelerating And Shaping The Financial Services Transformation Agenda During Times Of Change

Whether their focus is enterprise-wide, solutions-oriented, strategic or technical, the role of the architect in modern delivery projects is to thrive in the face of change, whether incremental or more abrupt

By Corneliu Rimboiu

COVID has forced us to adjust fundamental aspects of our lives with little warning and against a background of anxiety and uncertainty. However, while they test us, such dislocative events can also foster innovation and unlock opportunities.

Whether their focus is enterprise-wide, solutions-oriented, strategic or technical, the role of the architect in modern delivery projects is to thrive in the face of change, whether incremental or more abrupt. Modern architectures, design thinking, and ways of working are key success factors for each and any digital transformation journey. Modern architecture is about enabling your IT landscape to evolve iteratively, managing change holistically, and stimulating innovation.

The impact of remote working on the modern architect has been far greater than merely redefining the ways that language, messaging, diagrams, and concepts are packaged and communicated. Agile has already forced that transformation to happen. 'Just-in-time' architecture, cultivated by new ways of working, has already been adopted by our architects and continues to be embraced. Their role as facilitator and influencer has already evolved. Now it is time for soft skills to be redefined.

How can architects prepare for future changes?

1. **Get cloud architecture right:** The pandemic has (once again) highlighted the importance of a diligent and careful approach when architecting for cloud-based systems. It is preferable to embrace a host of models, patterns, and services rather than focusing solely on the public cloud. A highly scalable, dynamic, and extensible architecture – largely based on the same principles, no matter if 'on-prem', hybrid, or using its public version –is ideal. At CAPCO, we advocate laying down patterned code that is agnostic of infrastructure topology. Well-defined interfaces and standard protocols, complemented with a comprehensive DevOps pipeline, will allow a quick and reliable response to change.
2. **Modernize applications:** When it comes to 'demonolithing' legacy applications (such as a traditional client/server), an architect not only needs to have a deep grasp of both the new patterns and the legacy approach at all levels – logic, rules, and data. These elements will form the new services, with a view to establishing a fast-changing, scaling, and descaling ecosystem that adapts dynamically to meet demand.
3. **Harvest the power of data:** Beyond the super-computing power provided by the cloud, there is a need to address current data architecture concerns. Integrate siloed systems and normalize data access; and while maintaining a focus on security and privacy, redesign data architectures to allow moderated and controlled data mining. Looking forward, data will be generated on a whole new scale and will consequently require enhanced business intelligence and analytics.
4. **Evolve their own core skills:** The modern architect also has to keep up with the ongoing proliferation of architectural styles (microkernel, layered, n-tier, event-driven, microservices, space-based, serverless), as well as the plethora of new languages, cloud-native architectures, data architectures and security architectures. Last but not least, architects should be embedding themself within development teams and identifying and championing change.

The path forward

The lessons of history are instructive. For instance, the deregulation of UK markets ushered in by the 'Big Bang' of 1986 prompted a fundamental change in working and professional practices. It required a plethora of technology-backed support mechanisms to be architected and developed to facilitate a seismic transformation. Crucially, it also triggered a change in the consulting architect's language and toolset, and a variety of enterprise architecture frameworks were born during this decade: PRISM (1986), Zachman (1987) and NIST (1989).

'Just-in-time' architecture, cultivated by new ways of working, has already been adopted by our architects and continues to be embraced. Their role as facilitator and influencer has already evolved. Now it is time for soft skills...

We now find ourselves in a similar scenario, one that is at once immensely dislocative yet also rich with potential. As Albert Einstein noted, "In the middle of difficulty, lies opportunity". History has shown that there is always a winning path. By continuously and holistically assessing the readiness of your architecture to accommodate change, you will be better placed to identify that path – and in that context, modern architecture has a primary role to play in defining the future. ■

The author is Principal Consultant at CAPCO

Five Largest And Famous DDoS Attacks In History

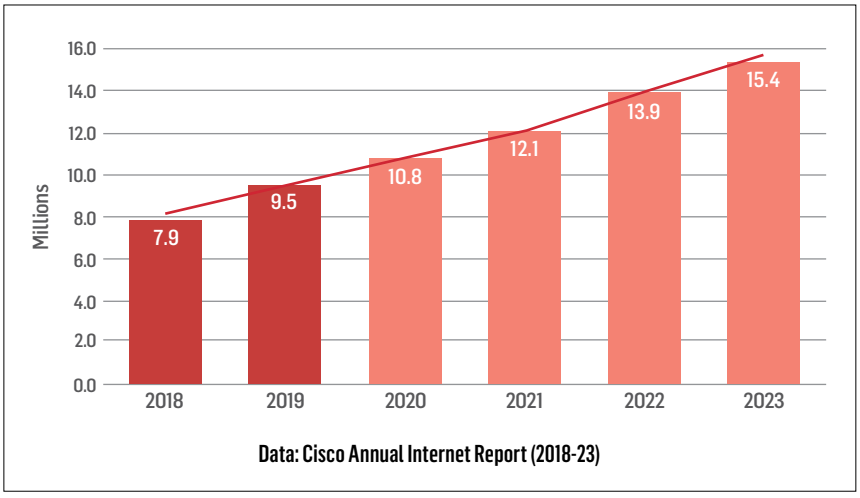
Over the next few years, DDoS attacks will become common and Cisco predicts that the total number of DDoS attacks will double from the 7.9 million seen in 2018 to something over 15 million by 2023

By Paul Nicholson

Distributed Denial of Service (DDoS) attacks are now everyday occurrences. Whether you're a small non-profit or a huge multinational conglomerate, your online services—email, websites, anything that faces the internet—can be slowed or completely stopped by a DDoS attack. Moreover, DDoS attacks are sometimes used to distract your cybersecurity operations while other criminal activity, such as data theft or network infiltration, is underway.

DDoS Attacks Getting Bigger, More Frequent

The first known Distributed Denial of Service attack occurred in 1996 when Panix, now one of the oldest internet service providers, was knocked offline for several days by a SYN flood, a tech-



Data: Cisco Annual Internet Report (2018-23)

nique that has become a classic DDoS attack. Over the next few years, DDoS attacks will become common and Cisco predicts that the total number of DDoS attacks will double from the 7.9 million seen in 2018 to something over 15 million by 2023.

But it's not just the number of DDoS attacks that are increasing; as the bad guys are creating ever bigger botnets – the term for the armies of hacked devices that are used to generate DDoS traffic. As the botnets get bigger, the scale of DDoS attacks is also increasing. A Distributed Denial of Service attack of one gigabit per second is enough to knock most organizations off the internet but we're now seeing peak attack sizes in excess of one terabit per second generated by hundreds of thousands or even millions of suborned devices.

The Cost of DDoS Attacks

Given that IT services downtime costs companies anywhere from USD 300,000 to over USD 1,000,000 per hour, you can see that the financial hit from even a short DDoS attack could seriously damage your bottom line.

The Top-Five Most Famous DDoS Attacks (for Now)

To give you insight, and not a small amount of fear, into what these attacks are like "in the wild," we're going to take a look at some of the most notable DDoS attacks to date. Our choices include some DDoS attacks that are famous for their sheer scale while our others are because of their impact and consequences.

1. The AWS DDoS Attack in 2020

Amazon Web Services, the 800-pound gorilla of everything cloud computing, was hit by a gigantic DDoS attack in February 2020. This was the most extreme recent DDoS attack ever and it targeted an unidentified AWS customer using a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) Reflection. This technique relies on vulnerable third-party CLDAP servers and amplifies the amount of data sent to the victim's IP address by 56 to 70 times. The attack lasted for three days and peaked at an astounding 2.3 terabytes per second.

Why the AWS Attack Matters

While the disruption caused by the AWS DDoS Attack was far less severe than it could have been, the sheer scale of the attack and the implications for AWS hosting customers potentially losing revenue and suffering brand damage are significant.

2. The Mirai Krebs and OVH DDoS Attacks in 2016

On September 20, 2016, the blog of cybersecurity expert Brian Krebs was assaulted by a DDoS attack in excess of 620 Gbps, which at the time, was the largest attack ever seen. Krebs' site had been attacked before. Krebs had recorded 269 DDoS attacks since July 2012, but this attack was almost three times bigger than anything his site or, for that matter, the internet had seen before.

The source of the attack was the Mirai botnet, which, at its peak later that year, consisted of more than 600,000 compromised Internet of Things (IoT) devices such as IP cameras, home routers, and video players. The Mirai botnet had been discovered in August that same year but the attack on Krebs' blog was its first big outing.

The next Mirai botnet attack on September 19 targeted one of the largest European hosting providers, OVH, which hosts roughly 18 million applications for over one million clients. This attack was on a single undisclosed OVH customer and driven by an estimated 145,000 bots, generating a traffic load of up to 1.1 terabits per second, and lasted about seven days. But OVH was not to be the last Mirai botnet victim in 2016...please see the next section.

Why the Mirai Krebs and OVH Attacks Matter

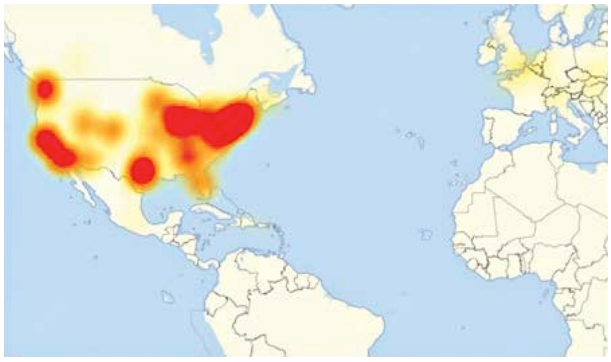
The Mirai botnet was a significant step up in how powerful a DDoS attack could be. The size and sophistication of the Mirai network was unprecedented as was the scale of the attacks and their focus.

3. The MiraiDynDDoS Attack in 2016

Before we discuss the third notable Mirai botnet DDoS attack of 2016, there's one related event that should be mentioned: On September 30, someone claiming to be the author of the Mirai software released the source code on various hacker forums and the MiraiDDoS platform has been replicated and mutated scores of times since.

On October 21, 2016, Dyn, a major Domain Name Service (DNS) provider,

was assaulted by a one terabit per second traffic flood that then became the new record for a DDoS attack. There's some evidence that the DDoS attack may have actually achieved a rate of 1.5 terabits per second. The traffic tsunami knocked Dyn's services offline rendering a number of high-profile websites including GitHub, HBO, Twitter, Reddit, PayPal, Netflix, and Airbnb, inaccessible. Kyle York,



Dyn's chief strategy officer, reported, "We observed 10s of millions of discrete IP addresses associated with the Mirai botnet that were part of the attack."

Why the MiraiDyn Attack Matters

Mirai supports complex, multi-vector attacks that make mitigation difficult. Even though the Mirai botnet was responsible for the biggest assaults up to that time, the most notable thing about the 2016 Mirai attacks was the release of the Mirai source code enabling anyone with modest information technology skills to create a botnet and mount a Distributed Denial of Service attack without much effort.

4. The Six Banks DDoS Attack in 2012

On March 12, 2012, six U.S. banks were targeted by a wave of DDoS attacks—Bank of America, JPMorgan Chase, U.S. Bank, Citigroup, Wells Fargo, and PNC Bank. The attacks were carried out by hundreds of hijacked servers from a botnet called Brobot with each attack generating over 60 gigabits of DDoS attack traffic per second.

At the time, these attacks were unique in their persistence: Rather than trying to execute one attack and then backing down, the perpetrators barraged their targets with a multitude of attack methods in order to find one that worked. So, even if a bank was equipped to deal with a few types of DDoS attacks, they were helpless against other types of attack.

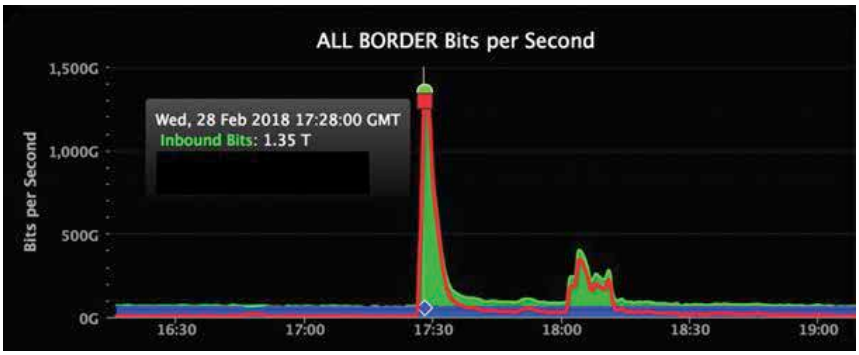
Why the Six Banks Attack Matters

The most remarkable aspect of the bank attacks in 2012 was that the attacks were, allegedly, carried out by the Izz ad-Din al-Qassam Brigades, the military wing of the Palestinian Hamas organization. Moreover, the attacks had a huge impact on the affected banks in terms of revenue, mitigation expenses, customer service issues, and the banks' branding and image.

5. The GitHub Attack in 2018

On Feb. 28, 2018, GitHub—a platform for software developers—was hit with a DDoS attack that clocked in at 1.35 terabits per second and lasted for roughly 20 minutes. According to GitHub, the traffic was traced back to "over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints."

The following chart shows just how much of a difference there was between normal traffic levels and those of the attack.



Even though GitHub was well prepared for a DDoS attack their defenses were overwhelmed—they simply had no way of knowing that an attack of this scale would be launched. As GitHub explained in the company's incident report: "Over the past year we have deployed additional transit to our facilities. We've more than doubled our transit capacity during that time, which has allowed us to withstand certain volumetric attacks without impact to users. Even still, attacks like this sometimes require the help of partners with larger transit networks to provide blocking and filtering."

Why the GitHub Attack Matters

The GitHub DDoS attack was notable for its scale and the fact that the attack was staged by exploiting a standard command of Memcached, a database caching system for speeding up websites and networks. The MemcachedDDoS attack technique is particularly effective as it provides an amplification factor – the ratio of the attacker's request size to the amount of DDoS attack traffic generated – of up to a staggering 51,200 times.

Other Notable Distributed Denial of Service Attacks

6. Occupy Central, Hong Kong DDoS Attack in 2014

The multi-day PopVoteDDoS attack was carried out in 2014 and targeted the Hong Kong-based grassroots movement known as Occupy Central, which was campaigning for a more democratic voting system.

A Distributed Denial of Service attack of one gigabit per second is enough to knock most organizations off the internet but we're now seeing peak attack sizes...

In response to their activities, attackers sent large amounts of traffic to three of Occupy Central's web hosting services, as well as two independent sites, PopVote, an online mock election site, and Apple Daily, a news site, neither of which were owned by Occupy Central but openly supported its cause. Presumably, those responsible were reacting to Occupy Central's pro-democracy message.

The attack barraged the Occupy Central servers with packets disguised as legitimate traffic and was executed using not one, not two, but five botnets and resulted in peak traffic levels of 500 gigabits per second.

Why the Occupy Central Attack Matters

It was reported that the attackers were probably connected to the Chinese government, there has never been conclusive proof and, perversely, the attack could have been intended to make the Chinese government look bad. The attack may have also provided cover for hackers who managed to extract Occupy Central staff details from a database to mount an extensive subsequent phishing campaign.

7. The CloudFlare DDoS Attack in 2014

In 2014, CloudFlare, a cybersecurity provider and content delivery network, was slammed by a DDoS attack estimated at approximately 400 gigabits per second of traffic. The attack, directed at a single CloudFlare customer and targeted on servers in Europe, was launched using a vulnerability in the Network Time Protocol (NTP) protocol which is used to ensure computer clocks are accurate. Even though the attack was directed at just one of CloudFlare's customers, it was so powerful it significantly degraded CloudFlare's own network.

Why the CloudFlare Attack Matters

This attack illustrates a technique where attackers use spoofed source addresses to send fake NTP server responses to the attack target's servers. This type of attack is known as a "reflection attack," since the attacker is able to "bounce" bogus requests off of the NTP server while hiding their own address and due to a weakness in the NTP protocol, the amplification factor of the attack can be up to 206 times, making NTP servers a very effective DDoS tool. Shortly after the attack, the U.S. Computer Emergency Readiness team explained NTP amplification attacks are, "especially difficult to block" because "responses are legitimate data coming from valid servers."

8. The SpamhausDDoS Attack in 2013

In 2013, a huge DDoS attack was launched against Spamhaus, a nonprofit threat intelligence provider. Although Spamhaus, as an anti-spam organization, was and still is regularly threatened and attacked and had DDoS protection services already in place, this attack—a reflection attack estimated at 300 gigabits of traffic per second—was large enough to knock its website and part of its email services offline.

Why the Spamhaus Attack Matters

The cyberattack was traced to a member of a Dutch company named Cyberbunker, which had apparently targeted Spamhaus after it blacklisted the company for spamming. This illustrates that companies and or rogue employees can mount DDoS attacks with immense brand damaging and serious legal consequences.

DDoS Attack Prevention with A10's DDoS Protection Solutions

Even though new types of Distributed Denial of Service attacks appear frequently, A10's Thunder Threat Protection System (TPS) employs advanced defense strategies that protect against all kinds of cyberattacks including new, novel DDoS attacks that could bring down your online and in-house services. ■

The author is Senior Director of Product Marketing, A10 Networks

Double Scoop

Two times the revelation

Amit Kumar

Senior Manager - IT, Manipal Health Enterprises

MY FAVOURITE POLITICIAN

Narendra Modi

MY FAVORITE CUISINE

Litti Chokha

A TECH SHOW I LOVE TO WATCH

Gadget Guru on NDTV

AN EMERGING TECH I WOULD LOVE TO USE THIS YEAR

AI/ML

MY FAVORITE CAR

Mahindra XUV300 W8

MY PEER IN THE IT COMMUNITY

Bhoopendra Solanki, Head - IT, Sakra World Hospital

Bhoopendra Solanki

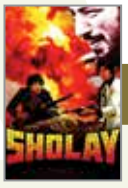
Head - IT, Sakra World Hospital

MY FAVORITE SOCIAL MEDIA PLATFORM

Facebook

MY FAVORITE AUTHOR

Munshi Premchand



MY FAVORITE MOVIE

Sholay

A WEB COMMUNICATION TOOL I USE THE MOST

Email

MY PASSION I WOULD LIKE TO PURSUE IN FUTURE

Build a completely digital hospital

To follow the latest in tech,
follow us on...

facebook.com/digitgeek

digit.in/facebook

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

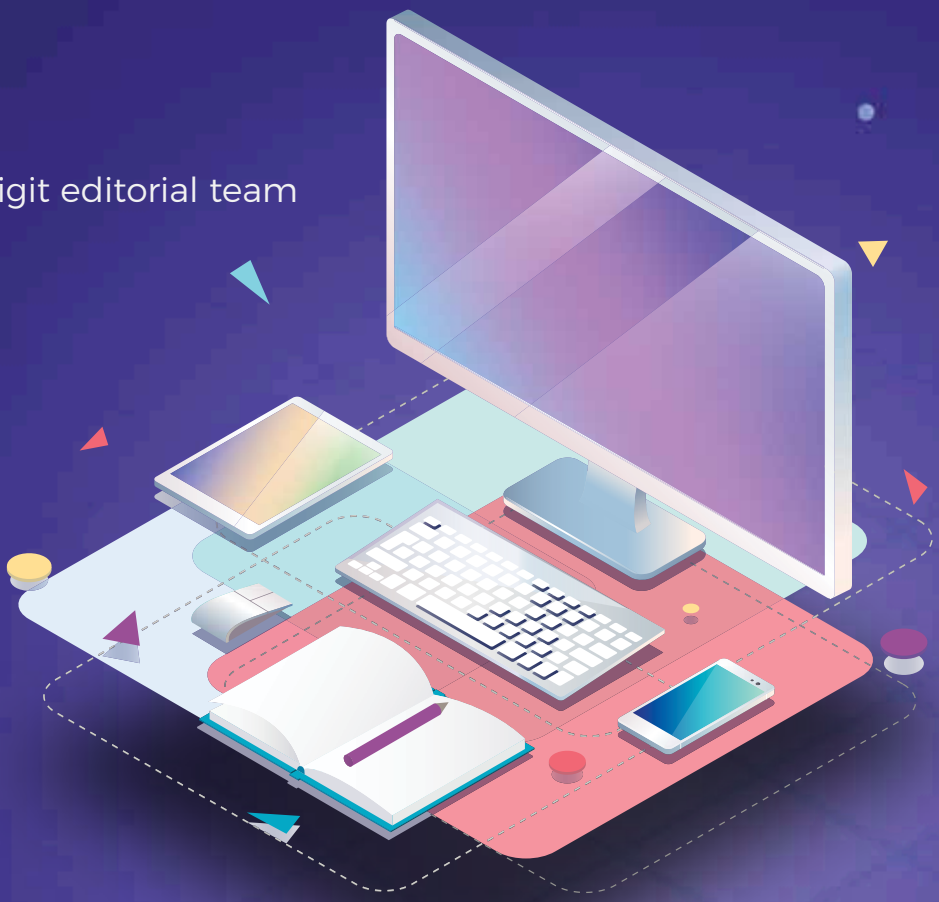
LAUNCHING

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

PAHWA GROUP
Innovation is life

SLOW POISONING

in Mission Critical Facilities like Data Centers may lower uptime due to breakdowns

SO_x

NO_x

H_2S

O_3

NH_3

VOC

Even low levels of air pollutants can corrode sensitive equipment over several weeks

DataCenter Air Purifier

EcoScrub

Bry-Air®

DataCenter Air Purifier

Neutralises corrosive gases

Remember, only air-conditioning is not enough.
Air-borne molecular contaminants from surrounding polluting industries, vehicular traffic, dump yards, open drains, etc. manage to seep into enclosed spaces and start corroding server cards, connectors and PCBs, leading to malfunction and interruptions.

Call us today to check the corrosive level in your facility.

BRY-AIR (ASIA) PVT. LTD.

Phone: +91-124-4184444 • E-mail: bryairmarketing@pahwa.com • www.bryair.com

RB/EA2023FCA3

Leaders in Gas Phase Filtration Systems