Security Special | Pg 12
Quantification Of Cyber Risk

Insight | Pg 26
Are You Ready To Move SAP To AWS?

ITNEXT

FOR THE NEXT GENERATION OF CIOs

POST-PANDEMIC IT INVESTMENT

Post-pandemic short/medium term IT investment plans have changed: **9.9 Group Research**

WHAT'S HOT?

- Quick tactical digitalization
- Cloud infrastructure services
- Laptops

WHAT'S NOT?

- Long-term transformation plans
- Own data center infrastructure
- Desktops

August 2020 | ₹100 | Volume 11 | Issue 05
A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

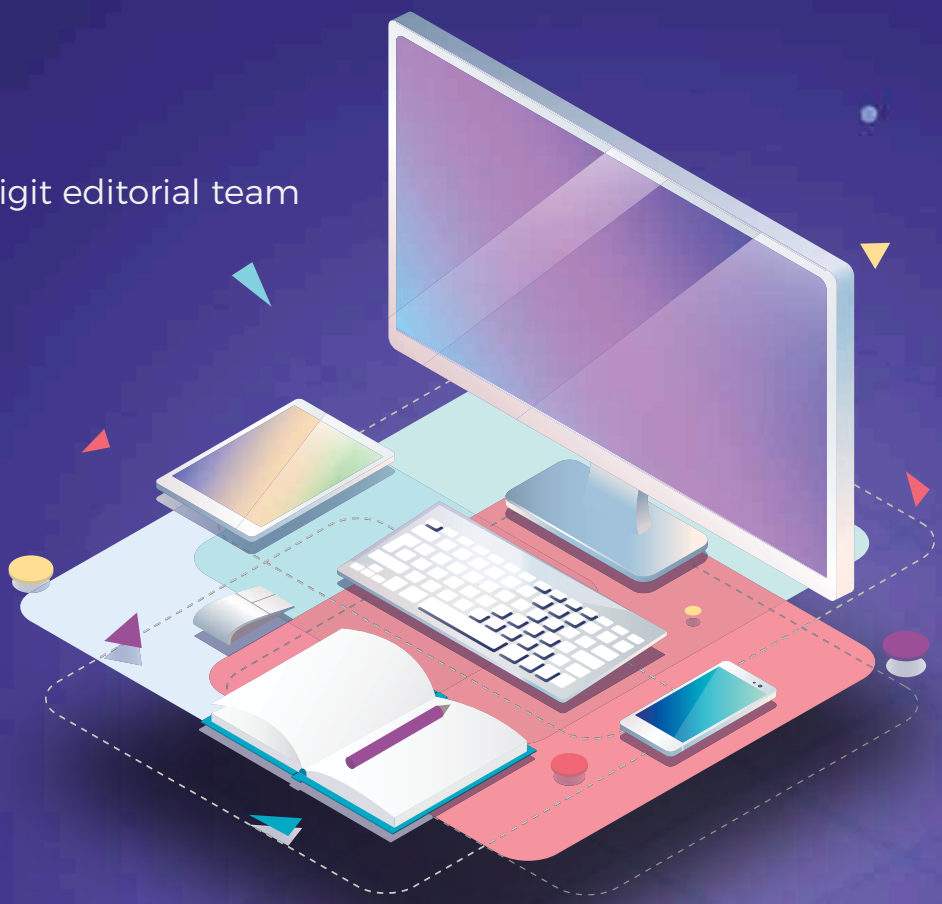
LAUNCHING

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

The Elusive New Normal

Sharing and collaboration among members of the IT community have increased significantly

Shyamanuja Das

Future is something that results from what we do today. The New Normal, by that logic, is not something that would come from another planet. It will be shaped by what we do today.

The enterprise IT managers, as the research presented in this issue shows, are not too sure about long-term planning, in the context of the post-COVID business. So, most of the long-term investment plans are put off, even though non-planned, but immediate digitization is happening across the organizations.

Meanwhile, we see technology companies presenting their own version of what the future could look like based on what technology solutions they have. Some of the common themes of course are business continuity, security, remote working, better application performance, contactless working and so on.

For the IT managers putting their money on one solution or the other is, of course, indirectly facilitating the movement in that direction.

However, of late, we see one emerging tendency. Instead of just doing a series of investments on technology, the IT managers have taken some kind of initiative to get their own insight. Since the trust on the long-term forecast is at an all-time low, many IT managers are trying to figure out what others are doing, share what they themselves are doing, asking for help and getting it too.

In short, sharing and collaboration among members of the community, have increased significantly. Since, most of the decisions are to do with immediate technology and product selection, limited implantation, quick learning and then extending it to a larger canvass, it is mostly the middle-level managers who are doing this.

In our NEXT100 WhatsApp groups, the new trend is explicitly and clearly visible.

It means a few new things:

- There's a forced agility about IT investments
- Power of community is being greatly realized and utilized
- Importantly, a lot of decision-making is now bottom-up
- Vendors are being listened to when they talk about immediate solution, not when they show distant future

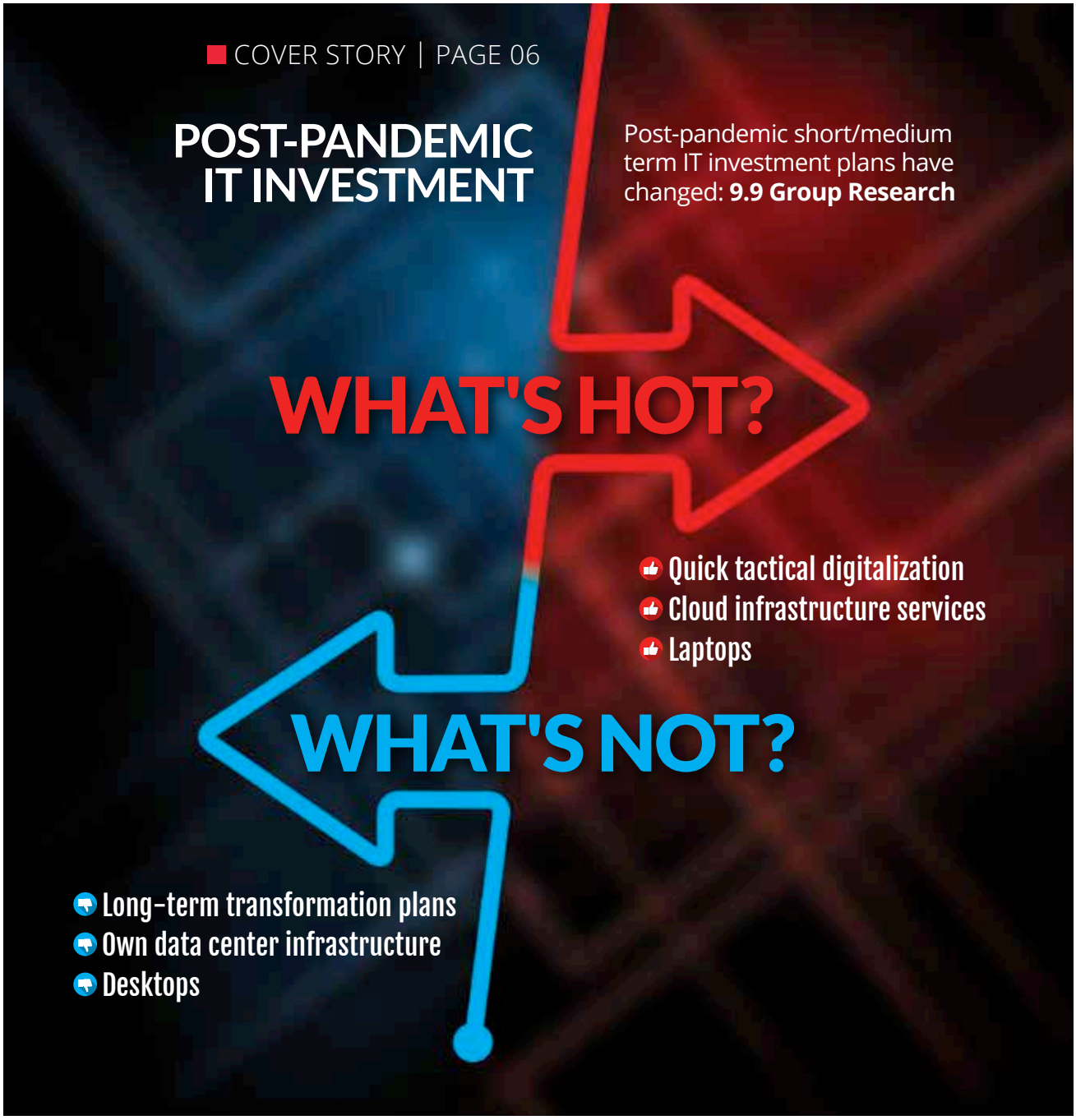
Many of these, if they continue for some more time, will, by themselves become the New Normal, that is so different from how it used to be, once upon a time. I mean six months back.

Don't look up for direction. Just look around for help from friends.

Like it or not, you are creating the New Normal. There is no other way. ■

AUGUST 2020
VOLUME 11 | ISSUE 05

Content



SECURITY SPECIAL | PAGE 12-14

Quantification Of Cyber Risk

SECURITY SPECIAL | PAGE 15-19

Security In The Virtual Workspace: Managing Cyber Risk In The New Normal

INSIGHT | PAGE 20-21

Rising Bot Attacks: Why Are Organizations Failing To Deal With Them

INSIGHT | PAGE 22-23

From Coronavirus To Cybersecurity: The Wisdoms Of Dealing With Pandemics

TRANSFAORMATION: A SECTORAL VIEW | PAGE 32-38

Retail And Hospitality

Cover Design:
BAIJU NV

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

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

EDITORIAL
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

Photography is a powerful language which speaks to us

Capturing Moments In Lights & Shadows

NEXT100 Winner 2017 **Amit Kumar,** Senior Manager - IT, Manipal Health Enterprises, reveals how photography has enabled him to view things differently and has given a whole new perspective...

Though I am not professional photographer but photography has always been my favourite hobby. It is sheer pleasure and relaxation, and refreshes the mind providing a welcome change from the busy routine of daily life. When I click pictures, it's like seeing things in a whole new perspective, literally and figuratively. It's not only the camera and the lens but a new perspective to see things. Photography made me realize that getting a different view of things means you have a more open mind to the world.

Almost every year I go on a short vacation along with my family. This is the time when I take most of my clicks. These clicks connect to our past, associate us with an event, and preserve memories without words or interpretation, which makes it an influential hobby for all of us.

When my friends invite me for parties or weddings, I usually take my camera along. If we happened to go on treks or hikes, I was there, ever ready with my inevitable camera. I am particularly interested in capturing landscapes, especially during twilight. I also began experimenting with lights and shadows.

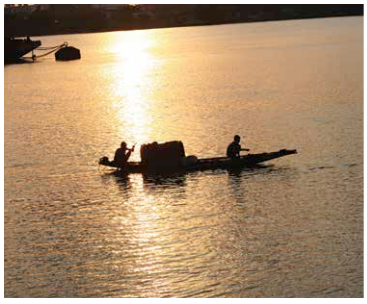
Photography has made my senses keen and my imagination sharp. I have developed a wonderful aesthetic sense. When I really have nothing to do, I just leaf through the photo albums and a whole gamut of interesting reminiscences rushes through my mind. Photography, at its best, is a powerful language which speaks to our emotions. It allows us to tell our story and show others our framing of the world around us. ■

As told to Dipanjan Mitra, Team ITNEXT

Amit Kumar

Snapshot

Amit Kumar is Senior Manager - IT at Manipal Health Enterprises. He has been a NEXT100 Winner in 2017. Earlier, he served in organizations like IMTAC and Escorts Heart Institute & Research Center, amongst others. He completed his Masters in IT and holds certifications in PMP & Business Analytics.




Inundating The Beauty Through My Lens

NEXT100 Winner 2017 **Abhishek Singh,** Solution Engagement & Delivery Head, Adani Wilmar, shares his immense passion for photography, automobiles and writing...

Putting words to pictures and pictures to words in between long drives and lazy explorations of life

I'm someone who loves to travel, captures things around through camera lens; prefers meeting people and having fun with friends. I take pictures of stories and write stories about pictures. My work across different locations has been a blessing for me to learn and understand various cultures and traditions and helped me pick the best out of these. I also learnt to appreciate diversity and accept differences in positive ways around me.

From my childhood days, life has been a journey and I have accepted everything which was presented by life to me as a blessing and tried not to miss any chance to follow my heart (during childhood) and passion (in later years), be it automobiles, photography and penning my thoughts in blogs.

The love for driving taught me to trust people and processes just like the mean machine (cars and bikes) before you can take it out for a drive and treat them at par with yourself. Photography taught me to have patience to wait and extract maximum out of the moment in life, as for that perfect moment to capture the shot. Writing helped me to bring the puzzle inside my mind to a simple language which can be consumed by everyone and intrigue the minds of the readers.

I prefer the journey rather than the arrival as I believe that if the journey is interesting, the end result will be satisfying too. While I am at it, I go without any plan and try to capture the random moments in between. It can be as small as green fields, a lazy sunset, a misty morning or a random person riding his bicycle as part of his/her daily chores. In these getaways, I enjoy and cherish little memorable moments with people, eat at roadside dhabas, have tea at small tea shops, have little chit-chats with them, learn about them and their lives. The collective experience from all these enriches me, rejuvenates me and makes me feel humble about the life around me, yet pushes me to give my best every day to the people and work so that I can make a difference in whatever I do on a day-to-day basis.

I clearly acknowledge and appreciate everyone who have been part of this journey called life and have made me the individual I am today.

To summarise myself in one line: "A nomad by choice, a geeky kid by profession!" ■

As told to Dipanjan Mitra, Team ITNEXT

Abhishek Singh

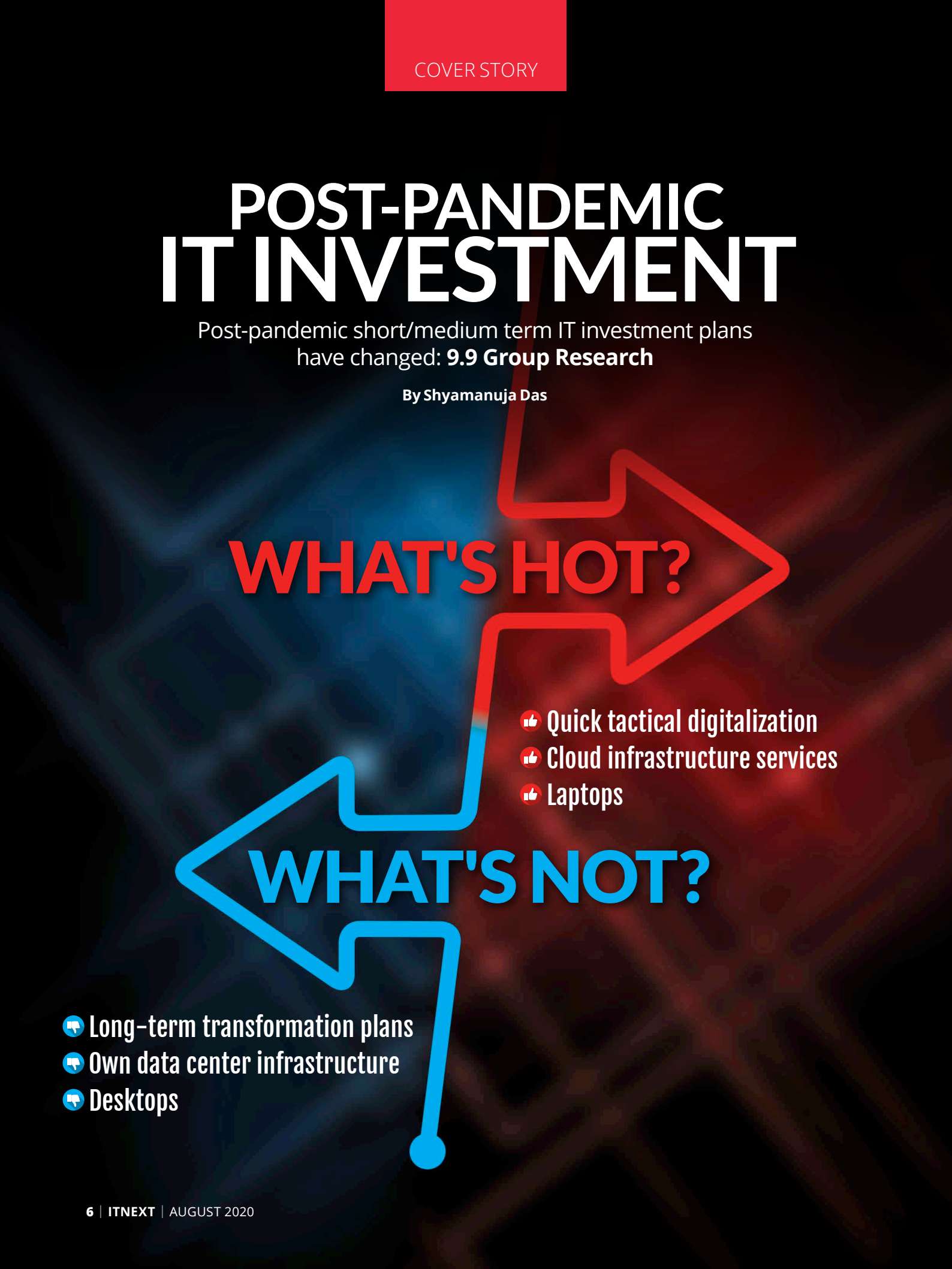
Snapshot

Abhishek Singh is Solution Engagement & Delivery Head at Adani Wilmar. He has been a NEXT100 Winner in 2017. Earlier, he had served in companies like Pernod Ricard, GSK Consumer Healthcare India, Reckitt Benckiser India, ITC Infotech India and Hindustan Unilever Limited. He holds a degree in MCA and a certification in ITILv2 Foundation from EXIN.

POST-PANDEMIC IT INVESTMENT

Post-pandemic short/medium term IT investment plans have changed: **9.9 Group Research**

By Shyamanuja Das



Every big disruption builds a new order. And we had not seen something like this for last six-seven decades.

You do not have to be a futurist to tell that things will change drastically post this pandemic. Some of it we have had a feel of—change in work, digitization of certain functions.

So, this story is about what would be those changes that would define what is being labelled the New Normal.

Sorry to disappoint. It is not.

It is easy to claim that we will show you the light to that elusive New Normal. Reality is: no one is sure. And we are not into tarots.

We can only tell you what you—that is you and your peers—tell us. And the big message from there—through a research that we conducted—is that people have still not started planning for that absolutely new normal. They are going one step at a time—agile method, if you like.

Corona surely has made the business executives—top managers to entry-level knowledge workers all included—'appreciate the value of digitalization.' But that is what it is.

Translating that appreciation/realization/enlightenment into action requires a few steps. And there are hurdles in the way.

First and foremost hurdle is the uncertainty about business. The way businesses worked in February 2020 and in June 2020—just four months apart—are completely different. The critical requirement for any long-term planning is some visibility into the planning period, which, today, is completely missing.

For years now, businesses have been talking of disruptive changes. Many companies also have had huge business continuity planning, largely focused on natural disasters or unrest. But the disruption that the pandemic brought, in terms of its nature and magnitude, had hardly been imagined.

While the technology fraternity, thanks to years of preparation, did a commendable job in responding to the new needs, it was to keep the wheels moving. The changes were for addressing immediate needs. It was a forced refresh. And some of the changes will stay. No one is sure—which ones and to what extent.

That is precisely why people have put a brake on all long-term plans. Our research, conducted in June-July, involving close to 60 senior-level IT decision makers in large enterprises, reveal that long-term plans are almost at the bottom of IT-investment priority—a tad better than only desktop purchase.

Second hurdle is the business situation. Almost all businesses have a huge cashflow issue. The economy was anyway in bad shape. It has gone worse, due to the pandemic.

While all businesses have seen severe cash crunch, some businesses—like airlines, hospitality, entertainment—have seen irreparable damage. So, most businesses do not have the money to invest, no matter how convinced they are about the ability of digital to make their business more effective, more efficient.

Last hurdle is the issue of budget allocation. Many organizations have invested—and that is what created this inflated positive hype—on digitalizing some functions, sub-functions or closed the non-digital gaps that remained in otherwise digitalized processes. These investments were not planned, at least not in the short run but they had to be made for making the businesses run. That was the bare minimum which kept businesses running. This was done at the cost of long-term plans which, anyway was risky because of the uncertainty.

The joke that the pandemic has driven digital transformation more than the CEO or CIO, is just that—a joke

So, the joke that the pandemic has driven digital transformation more than the CEO or CIO, is just that—a joke. Tactical digitization may have gone up but long-term transformational plans are the biggest sufferer when it comes to adjustment in IT investment priority, post pandemic.

The difference between the two is not difficult to comprehend. A transformational investment is targeted at changing business fundamentally, leveraging technology; a tactical digitalization is aimed at making something 'work' somehow.

Beyond a certain magnitude, no organization would make a series of tactical investments. For technology companies, all it means that unless the situation improved, business breadth may go—when large users make those investments in more geographies, more business functions—but the depth of digitization will have to wait till things become a little clearer and the cash situation becomes a little better.

When will that happen? Our guess is as good as yours.

But organizations will not just sit, as businesses move. CIOs have already reprioritized their IT investments. The research presented in this story

probed for just that. But unlike most of our other research, where we probe both short-term and long-term plans, we focused mostly only on investments in three months to 12 months—except one question where we asked them which business functions would see continued investment beyond 12 months.

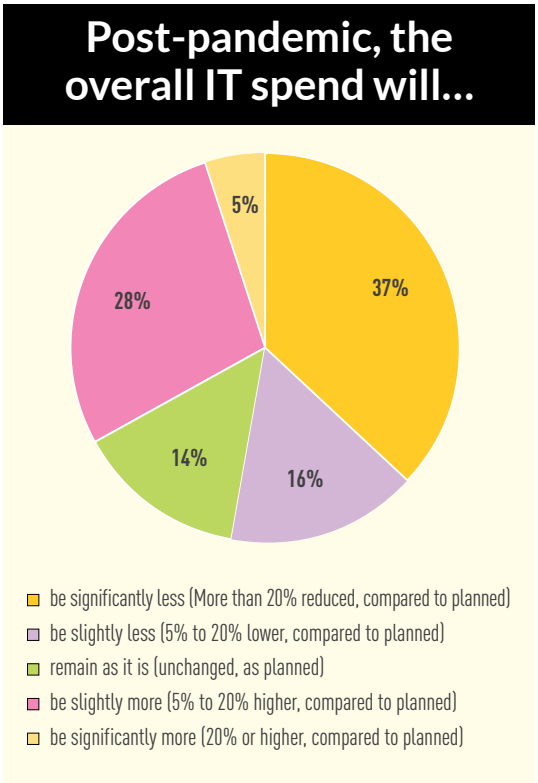
As Corona has reinforced the Tolstoyan thought about 'now' being the most important time, we present here the research findings that throw some light on the 'now' plans of IT managers in large enterprises.

The Big Question: Overall Investments

Only a third say overall IT investments in the post-pandemic scenario, in the next 3-12 months will be more than what was planned. That itself is anything but surprising. While 53% say the investments will be negatively impacted (which makes more sense intuitively), the pessimism is not showing when we asked them about individual investment areas.

In fact, in all but three areas—desktops, enterprise software and data center infrastructure—more than half the respondents said that investments will be somewhat positively or very positively impacted.

Post-pandemic, the overall IT spend will...



These two findings are contradictory. Right? How is it that the overall IT spend will be negatively impacted and most of the areas would see positive change? A technical explanation is that both enterprise software and data center account for the lion's share of enterprise IT investment. But again, the mood is also not too negative there; just that less than half of the respondents see those areas being negatively affected.

So, what explains this contradiction? Our off-the-record conversations with some CIOs gives some idea. (These conversations are not part of a formal research; so, we are not going to defend this; it is just some explanation; you can have your own theory).

"When you ask them about an individual area, they give you their assessment of the need—whether it will go up or go down. When you ask specifically about IT investment, the reality creeps in. And you know the reality," said a CIO in a large manufacturing company.

Another attributed this anomaly to "hope versus reality", essentially hinting at the same reason. Most others agreed that the impact will be positive but only when the situation becomes clearer. That is a big When....

What's In? What's Out?

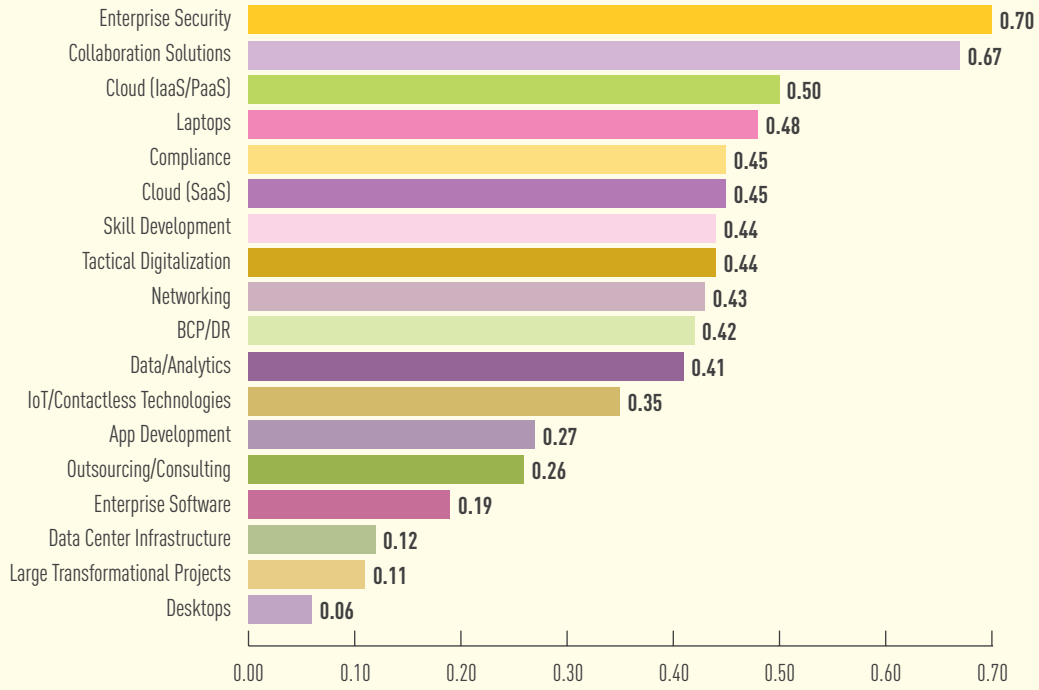
Any disruption creates a churn. And this disruption has no parallel in its depth and breadth. It has created both deep impact and is global. One unique attribute of this disruption is that it has made all of us—organizations, governments and people—technology savvy, in a matter of days.

It is but natural that organizations will rewrite their tech strategies. We tried to figure out how—albeit, only in the short to medium run, for reasons explained above.

And here are the findings. Respondents were asked how each of these IT investment areas be impacted in the next 3 to 12 months, separately. For easier comprehension and comparison with each other, we have reduced the findings of each technology area to an index—basing it on how many people said it would be positively (slightly or significantly) impacted, how many said it would be negatively (slightly or significantly) impacted and how many did not envisage a notable change.

Some of the findings are not difficult to guess—the focus on security, collaboration or cloud. They are the top things being talked about. Laptops too are essential for remote workers and is a natural tool for distributed working. Interestingly, what came as a surprise is that BCP/DR featured quite

How will each of these IT investment areas be impacted in the next 3 to 12 months?



low in the IT manager's list. Based on the comments left by the respondents and the CIOs we spoke to, something disturbing emerges: people have been let down by the current BCP/DR. While no one questions the effectiveness of technologies used, BCP is more about a plan than technology. And it did not deliver. People have spent huge money on protecting data centers and infrastructure from earthquakes, fires, water and through better planning of power and communications. But the plans did precisely little for the situation that arose in the wake of the pandemic. Data centers were hale and hearty. It is people who were stuck. Internet—that too public Internet—and Zoom/MS Teams/Webex/Google Meet saved the day for many organizations. Of course, it created new security challenges and organizations do want to address that.

Compliance is still fairly top of the mind and so is skill development. The latter probably is in an all-time highest position.

Enterprise software is an area that is almost towards bottom. While part of it may have come from a backlash which is evident in CIO conversations regarding some large software makers' inflexibility in a situation like this, this could also be because of a shift to SaaS, which is better for not just cash-flow, it suits a typical wait-and-watch situation.

Biggest loser, of course, are the long-term transformational projects. As discussed in the beginning, it is all about now, present and the immediate. No one knows how things will shape up. Tactical digitalization is significantly up, even though it does not show up at top. That is probably because many CIOs would not consider tactical. But the open-ended questions about priorities (see word clouds) point to a number of small digitalization activities.

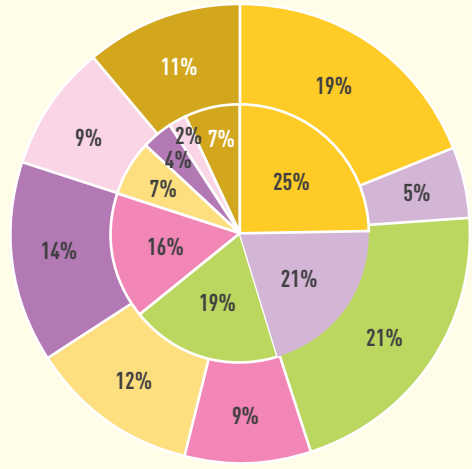
Priority for some of the pre-pandemic hot areas like data analytics has gone down significantly.

But these findings must be taken for what they are. They are short-term (three to 12 months officially, practically maybe three to nine months) plans. Long-term plans too will change. But no research can find that out now.

What part of business would be digitalized?

One of the most interesting findings is the difference in priorities in short-term and long-term

Digitalization of which business areas are priority?

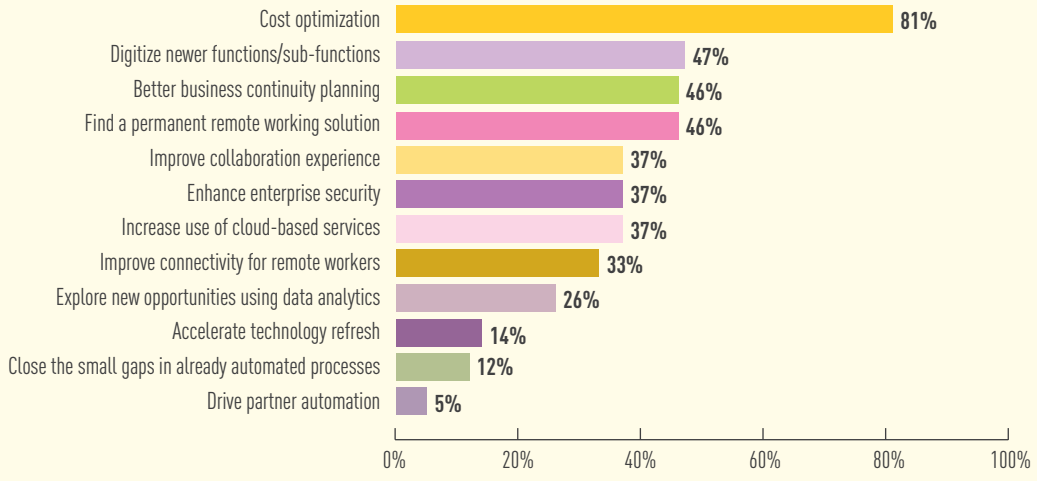


plans (only time we asked them about plans beyond 12 months) in specific business functions.

While Customer Service remains a top priority both in the short and long runs, Supply Chain, which is a big priority in the immediate future, next only to Customer Service, goes to the bottom of the table as a long-term priority. Supply Chain, which is a highly digitized area, most digitized in a manufacturing operation, had to be tweaked in the wake of COVID-19 to make certain approvals (which were still paper-based) digitized and certain processes contactless. But there is no major overhauling required. That is what probably takes the function off the list in the long run. Sales rises as the top digitization candidate in the long run.

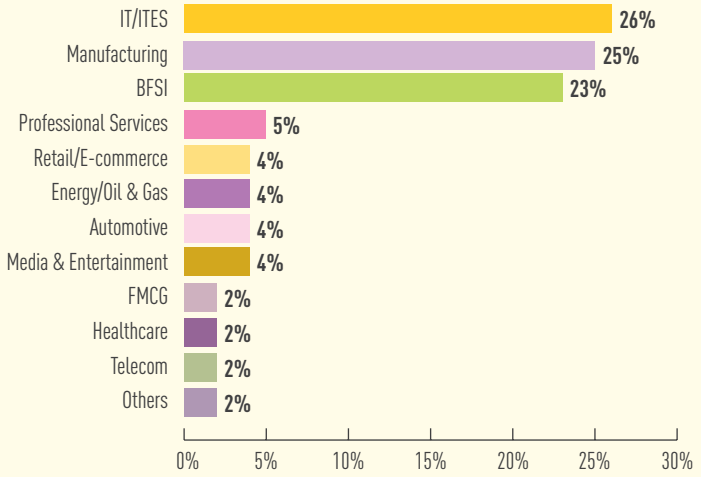
When asked specifically about areas that would see maximum digitalization in the short run, 'customer acquisition and management', 'customer experience', 'customer service', 'customer centric systems', 'customer engagement' featured predominantly. 'Processes automation', 'digitization of new processes', and 'supply chain analytics' and 'sales automation', 'employee experience' and 'employee engagement' also figured in the answers. The word cloud represents the most frequently used words in the answer to the question: list three specific sub-areas within each of the functional above areas where digitization efforts will be maximum in the immediate future?

What will be the biggest expectations from enterprise IT in the immediate/near term?

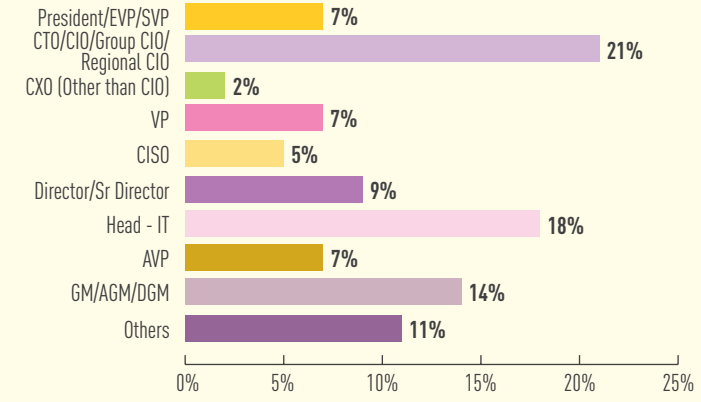


Respondents

INDUSTRY: IT/ITES, Manufacturing, BFSI represented 74% of the respondents, by and large reflecting the IT budget breakup among verticals



PROFILE: More than half of the respondents were president/SVP/EVP/VP/CIO/CXO/Director



Expectations from IT

Asked what are the expectations post the realization of digitization's value in the enterprise, most IT managers pointed to cost optimization. That is not surprising considering our research focused on the next few months' priorities. Most businesses are facing cash flow issues and are looking at cost optimization. CIOs are the best bet to help achieve that by streamlining processes.

On being asked what are the top three impacts on IT due to the change in business environment, most IT managers pointed to budget cuts. "Cut in overall IT budget", "controlled IT budget", "reduction in immediate spend", "hold on projects" were the most common responses. Close to half of the respondents agreed to have faced an IT budget cut or cost optimization. If there were budget cuts, there is also a push for more and more digitization. Of course, expectation on increased security and revamp of business continuity also came up as a factor that would impact IT significantly.

The word cloud summarizes the responses to this question.

The focus on short-term, cost optimization and tactical digitization of specific functions and sub-functions, all point to the cautious approach taken by the IT managers in the wake of uncertainty conditions prevailing post the pandemic.

Endnote

The biggest question that has not been answered by this research is—how it'll ultimately happen? Based on initial discussions with CIOs, we decided to leave it out, as including that for the sake of some numbers would not have done justice to the objective with which we had planned this survey—to give a realistic picture to the top IT managers and technology companies—and assess whether their problem is 'only their own' or the fraternity is facing the same challenges.

As things become a little clearer, we will surely supplement it with a long-term outlook research. Till then, you need to tell us how you are steering through these uncertainties.

Your experience is our data point. And our collective data point is your actionable insight. ■

Quantification Of Cyber Risk

Organizations can use Bayesian Data Analysis (BDA) for rigorous risk quantification and genuine decision support for risk management

By Venkatasubramanian Ramakrishnan

Organizations are increasingly realizing that the management of cybersecurity risk in complex environments needs to be addressed using suitable decision-making techniques. They are slowly embarking on the journey of quantifying their exposure to cybersecurity threats (operational risk) in much the same way they quantify credit and market risk exposure. While there is a wealth of data and well-established statistical methods for calculating credit and market risk, no such data or methods have been explored for quantifying cybersecurity risk.

Traditional Cyber Risk assessment methodologies generally use a likelihood/impact-based risk model to arrive at risk ratings. While useful as a starting point, such models suffer from serious deficiencies including:

1. Calculating the probability/impact is often oversimplified and may not put much thought into what lies under the hood.
2. Risk is not always independent. For example, speed of delivery and quality of delivery are always linked. Yet poor quality and missed delivery usually appear as separate risk factors in risk registers, giving the illusion that one can be controlled or mitigated independently of the other.
3. Visualization tools like heat map draws attention to the top right quadrant (high consequence and high likelihood), while items in other quadrants, especially low likelihood and high consequence risk, are generally ignored.
4. Risk scoring in traditional approach represents only one possible out-

come. In fact, operational risks can have a wide range of outcomes, i.e., a distribution of outcomes where each potential outcome has a corresponding probability.

5. Failure to addresskey concerns such as:
   a. What critical causal factors apply to specific risk factors.
   b. How to quantify risk reduction by implementing specific controls.

This article seeks to address these issues using a simple data analysis based on Bayesian Inference. Bayesian Data Analysis (BDA) brings together data, expert opinion, risk and uncertainty into a formal statistical framework, allowing decision-makers to see their choices clearly. Further, BDA can provide rigorous risk quantification and genuine decision support for risk management.

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)}$$

Bayes Theorem

Imagine this hypothetical, and simplified, scenario. As Security Head for company XXX, you have been called into the Executive Leadership discussion on the recent hack of one of your competitor'swebsitedue to specific vulnerability— huge data loss, reputation damage, and a lot of liability!

Executive Leadership: What is the chance that someone can hack one of our website and steal our clients' data?

Security Head: You pull out your Bayesian Hat and you say, "2.28% over the next year, but will update that number after penetration test."

Executive Leadership: We are always used to hear rank order terms like High, Medium etc. You seem to be coming out with a precise number. How did you arrive? As a follow-up question: How much will you change your probability if your test finds something? Or, what if your test finds nothing?

Calculation using Bayes Theorem

Based on the industry-based data breach report, your base rate (prior) for data breach is roughly around 2%.

What is the probability of data breach given penetration test is positive (vulnerable)?

What is the probability of data breach given penetration test is negative (not vulnerable)?

Now let us take that journey further into an interesting area, return on security investment (ROSI) using simulation.

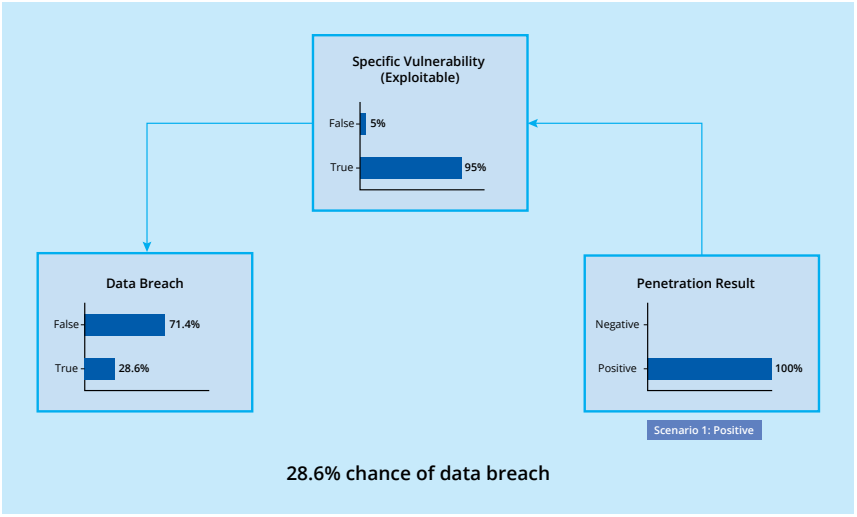
As Security Head for company XXX, you are proposing a new security investment to CFO for mitigation of specific risk event say malware at the cost of 25k USD/year (contrived example)

CFO: Fine. What is the likelihood of the risk event?

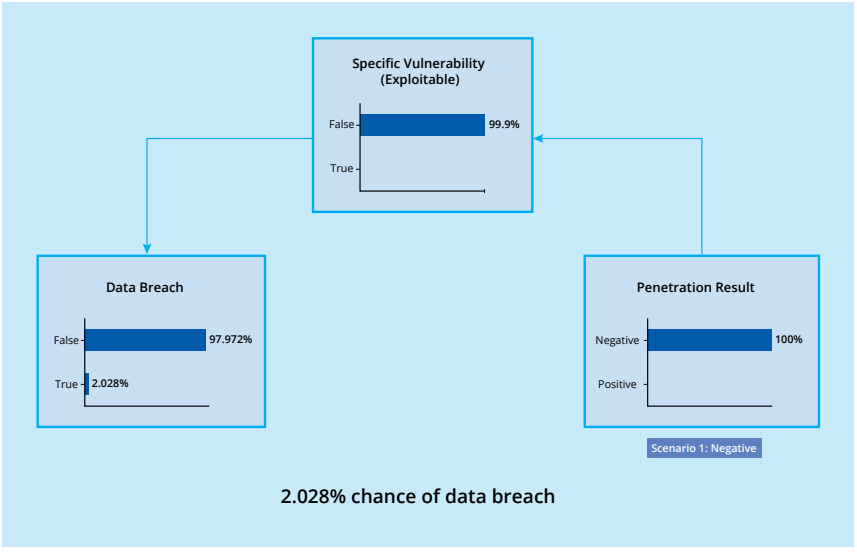
Security Head: You pull out your Bayesian Hat and you say, "20%"over the next year

CFO: Ok, great. Do we know the potential impact?

Security Head: Yes, I've discussed this with various Business and Functional Leaders to arrive at 90% confidence bound as

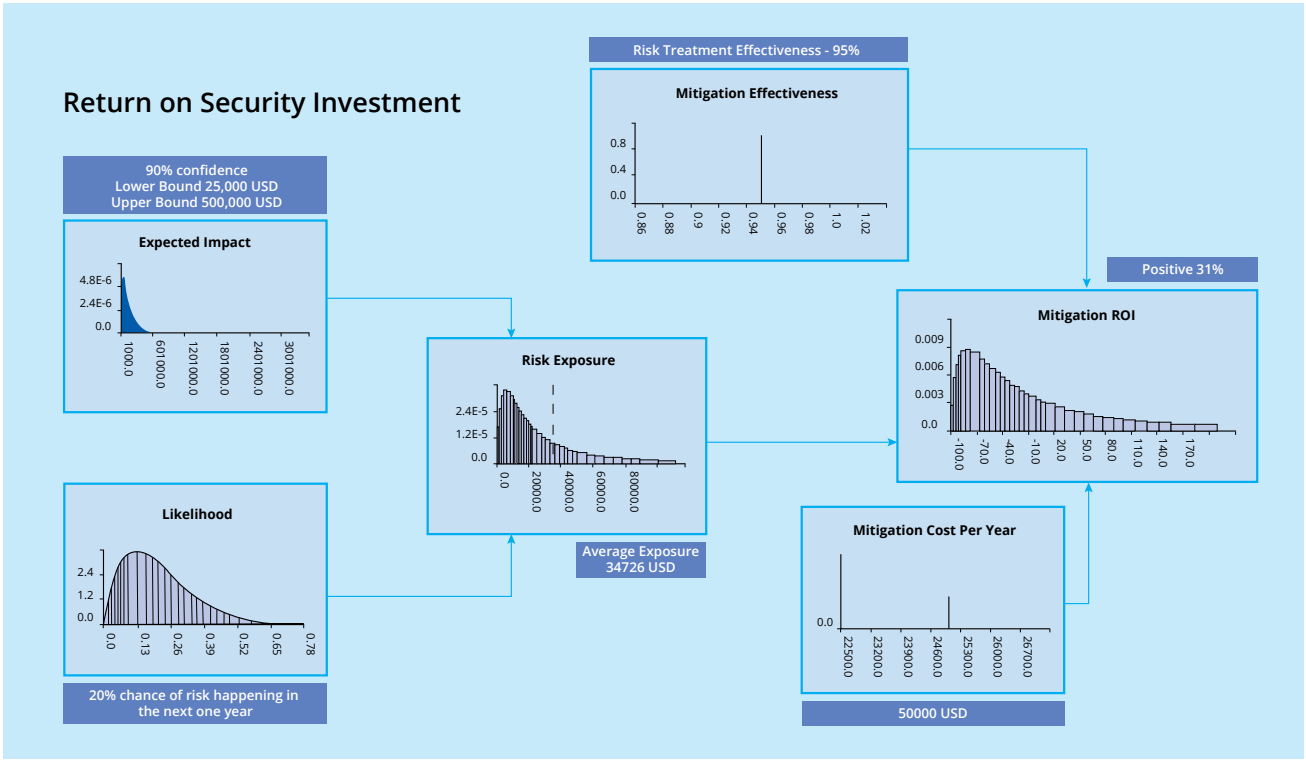


28.6% chance of data breach



2.028% chance of data breach

Isn't giving a definite probability better than saying simply High, Medium, etc.?



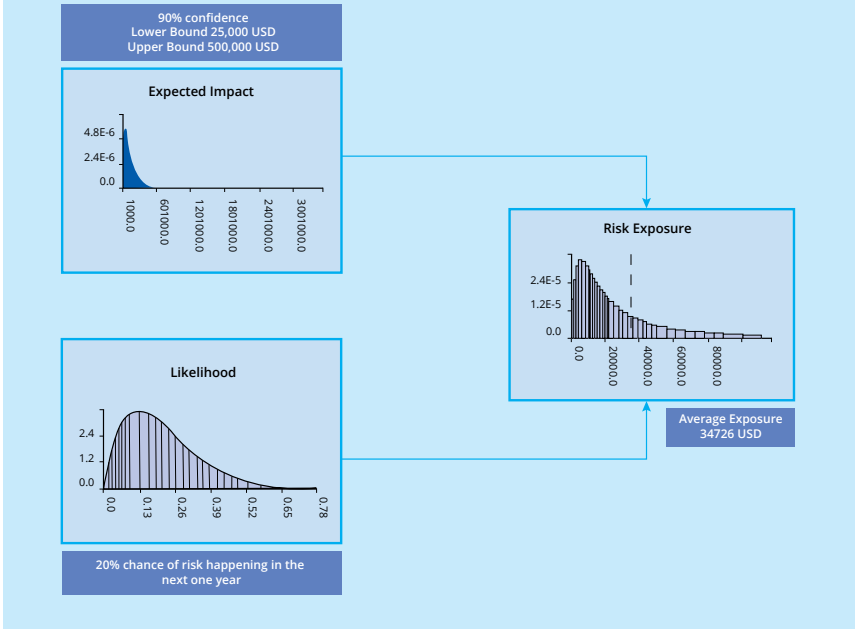
25k USD (Lower Bound)
500k USD (Upper Bound)

i.e. 5% chance that the impact may be less than 25k USD or greater than 500k USD. In other words, 90% likely there will be a loss equal to somewhere between 25k and 500k USD.

Key factors that we considered are legal fees, investigation fees, PR effort to convince clients, etc.

CFO: Ok, what is the average exposure?

Security Head: You pull out your Monte Carlo simulation tool and you say, "~35k USD" over the next year



CFO: Excellent. What is the Return on Investment (ROI)?

Security Head: It depends on how effectively we implement the mitigation strategy

CFO: Could you please explain?

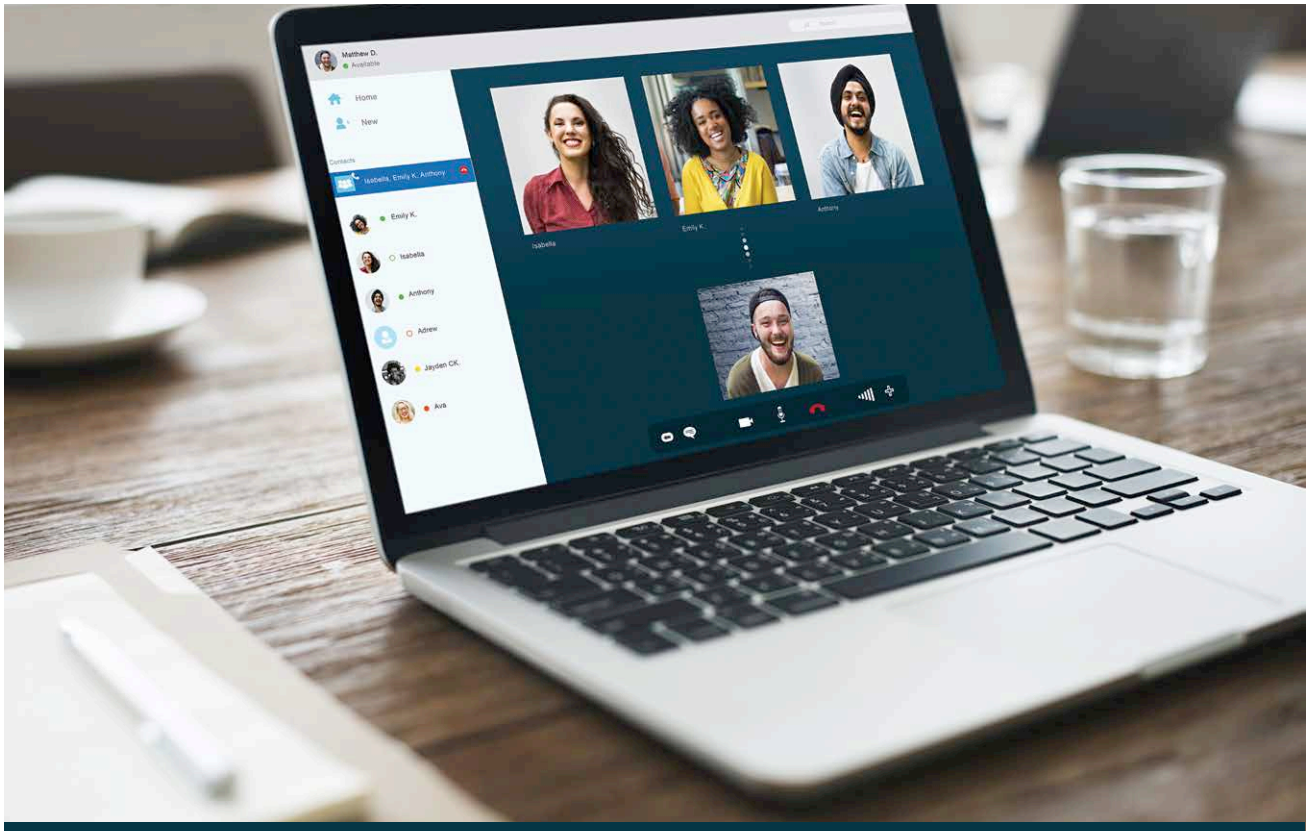
Security Head: You pull out your Monte Carlo simulation tool and you say, "negative 9%" over the next year if mitigation is only 40% effective and "positive 31%" over the next year if mitigation is 95% effective

Note: As a good practice, Security Head has to review the expected Impact and Likelihood as the context changes. Bayesian Philosophy is all about updating the belief based on new data.

Calculation

- Risk Exposure (RE) – Likelihood * Impact
- ROSI(%) – (RE * Mitigation Effectiveness - Cost of Risk Treatment Per Year*)/Cost of Risk Treatment Per Year ■

The author is Head - Cybersecurity, L&T Smart World & Communication



Security In The Virtual Workspace: Managing Cyber Risk In The New Normal

Resilience in the current scenario is a vital necessity. Businesses need to act on broader resilience plans as the shock begins to upturn established industry structures, resetting competitive positions

By Anuj Tewari

Risk Management is undergoing an evolution as we respond, reimagine and reform the operating model. At the forefront of enabling the new ways of operating, lie employee safety and ability to provide secure technology solutions to keep up with the new norms of working.

Working from home has changed the threat landscape for cyberattacks. Social engineering and vectors like phishing are rapidly on the rise. Malware delivery has accelerated as internet has become less restrictive with increase in use of BYOD (bring your own device).

Unlike the older days, where business continuity would typically be thought through at a building, facility, state or at a country level. With the

new working situation, the new continuity plans may morph to have working from home as the normal business operating state.

Dynamics of business relationships and partnerships would need to be re-thought along with third parties and vendors to maintain a resilient supply chain.

As workforce refocuses from dealing with here and now pandemic situation towards adapting new norms and ways of working, communicating creatively and often with focus and guidance on what to do, would be helpful. Increasing awareness of social engineering is going to be a key topic alongside, reiterating incident reporting and response protocols.

Organizations should rapidly review infrastructure and policies to support the new norms. Some of these aspects will play a critical role in creating a resilient workforce and ensuring availability of systems, which are needed to stay productive and help workforce embrace the new way we work.

Challenges Arising in Virtual Workspace

The impact of the COVID-19 virus is being felt by all businesses around the world. COVID-19 is affecting every element of business – from the robustness of supply to the availability of the labor force to the threat of rapidly waning customer demand.

However, there is no denying that it is also acting as a catalyst for change – economic, societal, personal, and corporate - on a scale not seen since World War II. And for all the uncertainty about what the future will look like, it is already clear that it will be digital. This pandemic has peaked the work-from-home trend. Millions of people have been transformed into remote workers overnight. Done right, remote working can boost productivity and morale; done badly, it can breed inefficiency, damage work relationships, and demotivate employees.

As organizations find ways to tackle the immediate response to this pandemic through processes re-alignment, controls framework, delivery structures and client expectations, there are some imminent risks that may not be easily apparent but require a risk management lens. "Predicting the unpredictable: dealing with risk and uncertainty" has always been a key mantra, and this holds true today with the emergence of COVID-19. There are many associated risks which are result of COVID-19, for example: cyber and fraud risks, reputation risks, supply chain risks, health & safety, to name a few.

There are some key challenges:

1. Dealing with cyber threats arising from work from home including threats like phishing, malware, ransomware, etc. and making an organization prepared to handle cyber incidents while working remotely.
2. Maintaining compliance with regulatory and governmental requirements, communicating changes and underlying decisions to stakeholders, financiers, regulators and staff.
3. Ensuring that capacity of collaboration tools and remote-working solutions copes with exceptional demand and adaptation of delivery team to new operating model and technologies.
4. Customer and employee personal data is safeguarded from leakage, theft and corruption even while working remotely and continuous compliance to data privacy regulations is maintained.
5. Addressing the need of individuals to feel safe, connected, engaged and motivated in order to continue working effectively. Further establishing robust communication mechanism to increase collaboration, transparency and build upon employee trust.

Let's get, in a little more depth, into the most important aspects of virtual workspace, through the lens of managing risk. They are:

1. Cyber Risk
2. Regulatory Resilience
3. Privacy
4. Technology and Collaborative Platforms
5. Operational Efficiency
6. Role and Context-based Service Enablement

1. Cyber Risk

While organizations are moving towards a virtual workplace to maintain service continuity, there is a need to ensure an adequate security posture is maintained and compliance is monitored. Security experts have found that large-scale remote working has led to a surge in phishing scams and other cyber threats for both individuals and organizations.

What is Virtual Workspace?

Virtual Workspace is an adaptive, scalable and connected environment with the combined force of social, mobile, cloud and analytics that helps retain productivity, deliver equitable experience and enables social distancing in borderless environment.

The virtual workspace has been constructed with the intention of enabling enterprise productivity with ease of access that fulfils next-gen workforce demands. In other words, it will focus, not on devices, but on users' productivity, along with the user experience.

Adaptive: Ability to adapt and cater to dynamic workspace needs

Scalable: Ability to scale the workspace and the workforce at will

Connected: Ability to connect the workforce and assets in any environment

Key objectives are:

- Empowers employees to work securely from anywhere and on any device
- Reduce risks of data breaches and ensure compliance with regulatory requirements
- Enhance cyber resilience so that organizations can quickly respond to and address cyber security threats

Let's look at the priorities.

Short-Term

- Ensure security operations teams are able to work remotely
- Impart awareness and knowledge on cyber risks such as phishing, malware and ransomware (provide coordinated cyber security advisories and announcements)
- Ensure active monitoring of the user behavior in the virtual workplace for security threats

Mid-Term

- Adopt zero-trust architecture in managing user identity and access
- Ensure cyber risks from virtual workplace are addressed adequately in the recovery strategies and crisis management plan
- Perform cyber risk assessments and revisit the cyber security strategy
- Establish detailed guidelines on securely collaborating, interacting and sharing sensitive data across various channels
- Enable security technologies around access, networks, end user, data security like DLP, SIEM, IDAM, PIM, etc.

Long-Term

- Automate cybersecurity operations to handle increased threats in order to avoid overloading security analysts
- Test and improve the robustness of established cyber security posture, including response to cyber threats such as advanced persistent threats, phishing and ransomwares

2. Regulatory Resilience

Regulatory resilience is the ability to continuously comply with applicable regulations even when working remotely. While establishing a virtual workplace, organizations should pay special attention to applicable regulatory requirements.

Key objectives are:

- Ensure compliance with applicable sectoral and regional/country regulations even in the face of a disaster
- People, process and technology that enable compliances to regulations are available seamlessly

Let's look at the priorities.

Short-Term

- Being diligent in keeping up with updates from regulatory bodies
- Identifying applicable sectoral and regional/country regulations and establish a process to comply the same
- Establishing appropriate communication channels for disseminating regulatory announcements or government advisories

Mid-Term

- Review current facility setup from a health and safety perspective and ensure that it meets applicable requirements from the regulators/ government agencies
- Review employment handbook, contracts and health insurance coverage to ensure compliance with regulatory requirements as well as contractual obligations towards employees

Long-Term

- Revisit the audit plan by continuing to maintain and demonstrate regulatory compliance, thus reducing the potential for scrutiny from regulators, which may interfere with or slow down business activities
- Review cross border contracts and transactions and the impact of regulatory changes in other countries
- Analyze process to comply with regulatory obligations under events which are beyond organization's control and considered as force majeure

3. Privacy

Teleworking requires several technology solutions. These tools are used to share and store personal information, confidential information and information towards which organizations have contractual and/ or legal obligations. To enable a virtual workplace, there is a need to consider how to collect, use and disclose personal information about employees/personnel in a privacy compliant manner.

Key objectives are:

- Increase the focus on data protection and ensure compliance to relevant data protection regulations
- Enabling and protecting access rights where personal information resides

Let's look at the priorities.

Short-Term

- Ensure that all communication channels offer adequate security for the protection of data being accessed and shared by moving to cloud VDI environment
- Consideration of just-in-time notice to allow employees/personnel to make an informed decision as to whether they want to provide the information requested
- Implementation of privacy by design for all new/ changes in technology, process and applications
- Restrict download of confidential information on personal devices
- Provide role-based access to employees to avoid misuse of personal information

Mid-Term

- Storage limitation- all personal data collected for the lawful purpose should be securely disposed or anonymized, and archived as per statutory/ regulatory requirements
- Collect and store personal and sensitive personal information in a

structured digital format, which will increase reusability of the data
- Implement data leakage prevention technology on all systems where personal information is accessed and stored

Long-Term
- Transfer of sensitive personal information within the country or abroad to be only permitted provided the receiver ensures the same level of data protection
- Adopt technologies to anonymize/ pseudonymize personal and sensitive personal information
- Automate activities such as personal information linking, breach notification, data discovery, consent management and vendor risk management

4. Technology and Collaborative Platform

Technology collaborative platforms form the core of a virtual workplace that enables employees to connect, collaborate and create more efficiently. Organizations have started acknowledging the need to invest in technology and infrastructure to support teleworking and virtual collaboration capabilities.

Key objectives are:
- Provide technology platforms that are simpler to adopt and easy-to-use to collaborate and connect
- Automate routine tasks of project management to help improve overall productivity
- Access to the knowledge base of the organization that enables employees to leverage existing information

Let's look at the priorities.

Short-Term
- Ensure that remote working capabilities are scaled up to handle a large number of devices
- Ensure that new policies and procedures are established, and resources are trained adequately to utilize collaboration platforms for remote working

While organizations are moving towards a virtual workplace to maintain service continuity, there is a need to ensure an adequate security posture is maintained and compliance is monitored

- Review helpdesk capacity for responding to queries from users
- Adopt holistic solution for collaboration

Mid-Term
- Leverage technologies such as cloud to enable flexible capacity planning
- Make use of intelligent technologies like self-healing platforms, etc.
- Define procedures and controls to ensure 24-hour platform availability for employees
- Provide adequate mobility to employees by enabling access via mobile applications (productivity and integration suites) and BYOD devices

Long-Term
- Automate helpdesk services utilizing process automation techniques
- Provide automation capabilities in knowledge management leveraging RPA techniques
- Review and reprioritize strategic technology investments and accelerate change programs that actively support resilience
- Embed data-driven culture to adapt and provide insights into changing customer needs
- Leverage augmented reality/ virtual reality to help collaborate better

5. Operational Efficiency

The paradigm of virtual workplace is all about improving the user experi-

ence through creating seamless and well-tuned workflows and generating efficiency benefits unparalleled in comparison to traditional workplace models.

Key objectives are:

- Addressing the need of individuals to feel connected, engaged and motivated in order to continue working effectively
- Meeting the operational needs of business even when facility is not available, delivering quality and meeting changing expectations of the customer
- Easier workflows to enable faster turnaround time

Here are the priorities.

Short-Term

- Standardize and centralize operations through digital solutions improving operational efficiency
- Understand where demand has fallen or increased and adjust workload across the workforce accordingly
- Implement agile models to adapt operations to the virtual workplace
- Focus on low hanging automation opportunities
- Accelerate RPA for routine tasks

Mid-Term

- Establish comprehensive metrics to measure and manage the efficiency of the digital workplace
- Integrated user management, IT services management and operations that work seamlessly to improve efficiency in the digital workplace
- Evaluate processes that can be automated to enable faster operations
- Build chatbots or self-service solutions that improve the efficiency of operations

Long-Term

- Reskill and/or upskill resources to enhance their versatility across different functional capabilities
- Continuously improve the operations by leveraging data and analytics
- Revisit the design of the employee remote experience to account for the new normal

6. Role and Context-based Service Enablement

In the work from home model, it becomes very crucial that employees have access rights to only the information/information systems that they require to do their jobs. Further, other contextual parameters like location, time of the day should also be considered while providing access rights.

Key objectives are:

- To safeguard the organization from fraud and data leakage by ensuring access is provided only on a need-to-know basis considering the business role of the employee and location
- Effective governance management to monitor and restrict any malicious access

Let's look at the priorities.

Short-Term

- Standardize roles and associated responsibilities
- Define rules for granting access rights in a virtual workplace, including establishing contextual parameters that should be considered, such as location, role, and time of the day

Mid-Term

- Evaluate and redesign processes to enable role-based access
- Update architecture to align with redesigned processes to ensure role-based access
- Perform role-based access rights reconciliation and identify discrepancies

Long-Term

- Automate role-based access and tagging of users to specific business functions
- Making use of user behavioral analytics tools like UIBA to identify fraudulent behavior and accordingly reduce/remove privileges

Managing Risk inVirtual Workplace: Need for a Holistic Approach

Resilience in the current scenario is a vital necessity as businesses need to act on broader resilience plans as the shock begins to upturn established industry structures, resetting competitive positions. In order to effectively recover from the crisis and embrace the business opportunities that may arise from disruptions caused, organizations should focus on the following critical areas:

- **Realign Cyber Resilience:** Realign cyber posture to enable Anytime, Anywhere Workforce. Enhancing programs to identify, detect, protect and respond to the cyber threats in a zero-trust security model.
- **Resilience:** Meet the operational needs of business even when facilities are not available, delivering quality and meeting changing expectations of the customer. Authorized personnel can access the right technology from anywhere, anytime with any device to remain productive.
- **Focus on Regulatory Compliance:** Maintaining trust through global disruptions by building confidence in business to respond to changes in regulatory and contractual requirements.
- **Privacy by Design:** Increased focus on data protection and ensure compliance to relevant data protection regulations. Enabling and protecting access rights where personal information resides.
- **Digital Transformation:** Provide technology platforms that are simple to adopt, easy to collaborate and connect. Drive efficiencies by enabling technologies like cloud, AI, machine learning and data analytics.
- **Culture and Employee Wellbeing:** Recalibrate the culture to thrive in the new normal. Encourage a people-positive approach through collaboration and teamwork. ■

The author is CISO, HCL Technologies

Rising Bot Attacks: Why Are Organizations Failing To Deal With Them

Bots are being used to take over user accounts, perform DDoS attacks, abuse APIs, scrape unique content and pricing information and more

By Nikhil Taneja

The need for bot management is fueled by the rise in automated attacks. In the early days, the use of bots was limited to small scraping attempts or spamming. Today, things are vastly different. Bots are being used to take over user accounts, perform DDoS attacks, abuse APIs, scrape unique content and pricing information and more. In its "Hype Cycle for Application Security 2018," Gartner mentioned bot management at the peak of inflated expectations under the high benefit category.

Despite serious threats, are enterprise businesses adopting bot management solutions? The answer is NO. Many are still in denial. These businesses are trying to restrain bots using in-house resources/solutions, putting user security at risk. In a recent study, Development of In-house Bot Management Solutions and their Pitfalls, security researchers from Shield Square found that managing bots through in-house resources is doing more harm than the good.

Against 22.39% of actual bad bot traffic, advanced in-house bot management solutions detected only 11.54% of bad bots. Not only did these solutions fail at detecting most of the bad bots, but nearly 50% of the 11.54% detected were also false positives.

So why do in-house bot management solutions fail? Before we dive deeper into finding out the reasons behind the failure of in-house bot management solutions, let's look at a few critical factors.

More Than Half of Bad Bots Originate from the U.S.

As figure 2 shows (see below), 56.4%

of bad bots originated from the U.S. in Q1 2019. Bot herders know that the U.S. is the epicenter of business and showing their origin from the U.S. helps them in escaping geography-based traffic filtration.

For example, many organizations that leverage in-house resources to restrain bots often block the countries where they don't have any business. Or, they block countries such as Russia, suspecting that's where most of the bad bots originate. The fact is contrary: Only 2.6% of total bad bots originated from Russia in Q1 2019.

Cyber attackers now leverage advanced technologies to sift through thousands of IPs and evade geography-based traffic filtration. When bots emanate from diverse geographical locations, solutions based on IP-based or geographical filtering heuristics are becoming useless. Detection requires understanding the intent of your visitors to nab the suspected ones.

One-Third of Bad Bots Can Mimic Human Behavior

In Q1 2019 alone, 37% of bad bots were human-like. These bots can mimic human behavior (such as mouse movements and keystrokes) to evade existing security systems (Generation 3 and Generation 4 bad bots, as shown in figure 3).

Sophisticated bots are distributed over thousands of IP addresses or device IDs and can connect through random IPs to evade detection. These stealthy detection-avoiding actions don't stop there. The programs of these sophisticated bots understand the measures that you can take to stop them. They know that apart from random IP addresses, geographical location is another area that they can exploit. Bots leverage different combinations of user agents to evade in-house security measures.

In-house solutions don't have visibility into different types of bots, and that's where they fail. These solutions work based on the data collected from internal resources and lack global threat intelligence. Bot management is a niche space and requires a comprehensive understanding and continuous research to keep up with notorious cybercriminals.

Organizations that are working across various industries deploy in-house measures as their first mitigation step when facing bad bots. To their dismay, in-house solutions often fail to recognize sophisticated bot patterns. ■

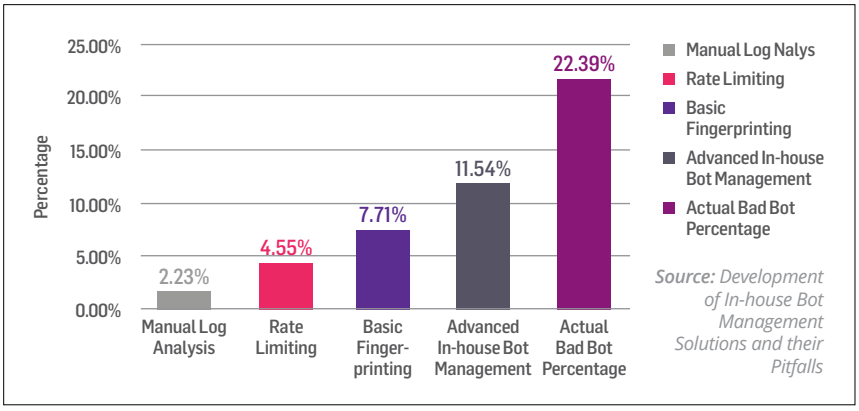


Figure 1: Bots Detected by In-house Bot Management Solutions vs. Actual Bad Bot Percentage

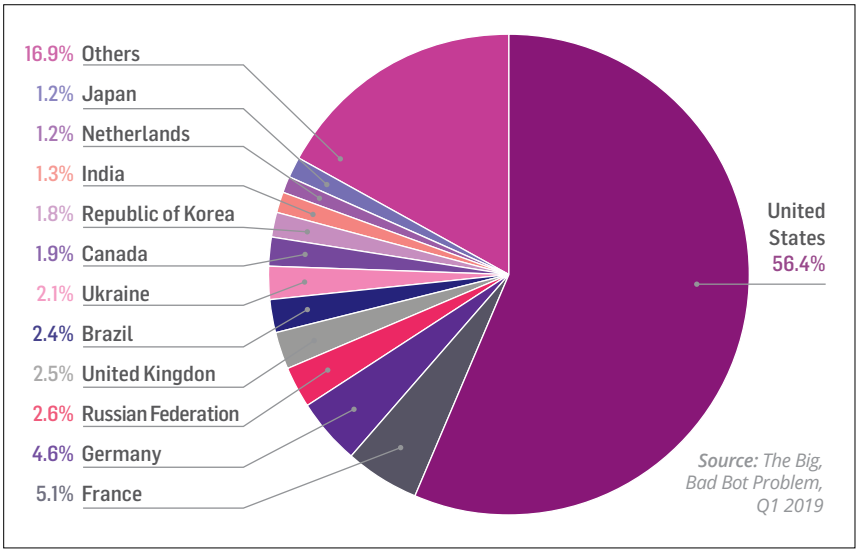


Figure 2: Origin of Bad Bots by Country

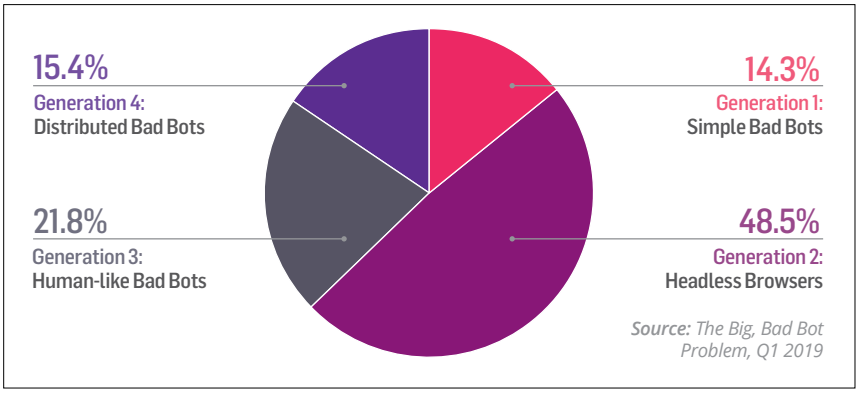


Figure 3: Bad Bot Traffic by Generation

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

From Coronavirus To Cybersecurity: The Wisdoms Of Dealing With Pandemics

COVID-19 will go away, just like any of the pandemics in the past. But cyberattacks will stay as long as there's a computer connected to the internet

By Dhanya Thakkar

In the span of a few months, the coronavirus has reached every country, every community, and every neighbourhood. No nation is spared. Economy grinds to a halt. Millions have fallen sick.

In the meantime, if you take a look at the 15 biggest cyberattacks in the 21st century, you'd notice a few things. First, no country is untouched. Second, it's extremely disruptive to business operations. Third, millions have fallen victim to these attacks. We have been dealing with a different kind of outbreak for many years, that is, the pandemic of cyberattacks.

The world responds

By now, most countries have imposed a mixed bag of measures to deal with the outbreak. If you look closely, the overarching strategy for dealing with COVID-19 has revolved around four quadrants: prevention, detection, response, and prediction.

In cybersecurity, we often talk about the importance of a holistic strategy that consists of the same quadrants. At its core, a good cybersecurity strategy should take

multi-pronged approach and a long-term view.

Prevention

The first pillar of the defense is prevention. In the time of COVID-19, prevention means protecting people from being infected in the first place, such as washing your hands, socially distancing yourself from others, disinfecting your phone and wallet when you get home, and more.

In cybersecurity, prevention means the exact same thing – protecting your IT assets from being infected in the first place. Because most major data breaches can be traced back to a single point of failure that could have been prevented.

Today, many new cybersecurity vendors talk of a shining silver bullet that miraculously waves away all your cybersecurity headaches – such as machine learning or EDR. But in reality, the concept of a single silver bullet doesn't hold up. You need the basic technologies – such as antivirus, application control, web and file reputation, etc. – to do the heavy lifting. These technologies can filter majority of the alerts, categorising them as either good or bad.

Detection – knowing what you're looking for

Contact tracing is crucial during outbreaks. The longer you take to identify a patient, the more people will be infected.

In cybersecurity, detection is about the same thing – how fast you can detect a breach in your system determines the scope of damage. We believe in this strategy called connected threat defense. By deploying security solutions at all the touchpoints in an IT system, from the endpoints to the network to the server, you can start to connect the dots and gain visibility into every nook and cranny. If you know what's lurking in your IT environment, you can significantly increase your chance of getting rid of it.

Endpoint detection and response (EDR) is another tool designed for the same purpose. EDR technology works like a black box in a plane. It records everything that takes place on the endpoints and threat hunters can rewind to see from which point a threat entered the system, and how it spread across the network. Based on the information, a blueprint of the malware's infection path can be drawn.

Today, many new cybersecurity vendors talk of a shining silver bullet that miraculously waves away all your cybersecurity headaches...

Response – prioritizing the important ones

During the outbreak, there are many false positives and false negatives. Some people may test negative now but develop the symptoms next week. Suspected cases may turn out to be totally innocuous. Because the medical supplies are limited, the healthcare workers need to prioritize. To prioritize, you need context-rich information about the patient.

It's the same in cybersecurity. A security operations center (SOC) receives thousands of alerts on a daily basis. Hence, prioritization becomes the key and this is where XDR comes into picture. XDR is the natural progression from EDR. The X stands for anything you can apply detection technology to, such as emails, servers, or the network. XDR is a big collector of security alerts, absorbing data from various touchpoints.

Essentially what XDR does is to break the silos between all these solutions gathering data on their own. A prominent feature of the XDR tool is a central data lake where all data will flow to eventually and be analysed as a collective.

All this data churning can minimize alert fatigue, as it produces high-priority alerts with rich context around it. SOC analysts can now focus on alerts that need immediate action instead of combing through every single one of them and manually looking for connection.

Prediction – taking two steps ahead

Wall Street Journal reported that epidemiologists were teaming up with data scientists to forecast the spread of the coronavirus outbreak in the near future. By taking into consideration a vast array of different types of data, the model is expected to predict the number of new cases to arise in an exposed population, or peak infection rates.

Likewise, in cybersecurity, the more accurate our predictions are, the more effectively we can deal with an upcoming data breach. We achieve this by collecting and correlating a vast array of different types of detection and activity data from our native sensors, deployed at different layers within the organization, like the endpoint, network, email, and the cloud environment.

Combined with big data analytics, threat models, advisory-based behavior analytics and detection rules from our security experts, we can help to uncover if an emerging or unknown threat or a threat actor is attempting to infect your organization. On top of that, continuous risk assessment of an organisation's cybersecurity posture also serves to predict impending issues.

COVID-19 will go away, just like any of the pandemics in the past. But cyberattacks will stay as long as there's a computer connected to the internet. The most effective way to deal with cyberattacks is not to dream of a cure-all panacea, but to take small but coordinated measures that culminate in an all-rounded defense strategy. ■

The author is Vice President & Managing Director, AMEA, Trend Micro

OT Security Breaches Are Anything But Rare

For the last couple of years, the breach rate has risen to 80%, illustrating that OT systems are indeed cyber adversary targets of primary interest

By Rajesh Maurya

Across industries, owners and operators of Critical Infrastructure (CI) continue to converge the cyber and physical aspects of their businesses. This merger has enabled more efficient and effective monitoring of critical processes, as well as the ability to virtually leverage data from enabled sensors, industrial applications (including robotics), medical devices, and software-defined production processes. This range of capabilities, better known as the Industrial Internet of Things (IIoT), assist decision making in real-time and ensures significant cost savings in terms of power consumption and employee efficiency.

Despite these benefits, organizations must also understand the potential security risks they are facing as IT and Operational Technology (OT) departments and their respective support systems converge. Without an effective OT security plan, ICS/SCADA systems are left vulnerable to cyberattacks that could result in financial loss, reputational damage, diminished customer confidenceand even threaten the safety of citizens and national security.

OT-hosted ICS/SCADA Systems Are Being Exposed to New Threats

The need for protecting OT enterprise and integrated ICS/SCADA systems can hardly be understated. There is an absolute dependence on safe and sustained operations that span everything from Manufacturing to Energy and Utilities to Transportation infrastructure – these OT vertical sectors comprise and deliver a range of services that citizens around the globe count on daily. The advent of executive-level commitment to digital transformation strategy and propor-

tional operational efficiency gains has materialized a significant range of cybersecurity concerns as these historically air-gapped systems are now exposed to cyber risks and a broader attack surface.

The commitment to OT system efficiency, in turn, raises the bar for OT Security standards, making it more difficult than ever for organizations to adequately protect their high-value cyber-physical assets. With this in mind, Fortinet and Forrester have come together for a third time to survey industry leaders who manage and maintain OT infrastructure. Overall, the purpose of the report is to identify and illuminate the security trends and practices that impact operations and demand security strategy and investment.

Here are key findings from the latest report.

OT Security Breaches Are Anything But Rare

OT security breaches are taking place at distressing rates. Among those surveyed for this study, only 10% reported that they have never experienced this type of threat. In contrast, 58% of organizations surveyed have had a breach in the past 12 months and as a result, more than three-quarters expect regulatory pressure to increase over the next two years. In fact, if you expand the period of consideration to 24 months, the breach rate rises to 80%, illustrating that OT systems are indeed cyber adversary targets of primary interest.

It is no surprise, then, that there has been a strong drive to commit greater resources on security – 78% plan to increase their ICS/SCADA security budgets this year.

Organizations Are Moving Purposefully Toward IT-OT Convergence

OT systems traditionally thought to be "hardened" by an air-gap are often built upon legacy software, and hardware and life cycles can be measured in decades. Naturally, one significant take away from the move to converge IT and OT networks is the expansion of an attack surface that enables access to an environment where vulnerabilities exist. Indeed it is the very pursuit of operational efficiency through IT/OT convergence that resulted in broad connectivity and exposure to more traditional IT threats. This connectivity not only brings added risk but more likely opens the door for cybercriminals in a way that was not possible when these systems were isolated.

Concerns over the complexity of converged IT/OT systems were also noted in the survey. Almost all respondents (96%) foresee challenges as they move toward convergence, resulting in deliberate, careful movements that center on concerns around security. Among the respondents, more than one-third reported worrying about the following OT security challenges:

1. Third parties lack security expertise needed to assist with converged technology and the Internet of Things (IoT)
2. Sensitive or confidential data will be leaked
3. In-house security teams lack the expertise required to secure converged technology and the IoT
4. Connected smart devices will cause breaches
5. Organizations have trouble staying current with the latest security tactics and protocols
6. If and when a breach occurs, organizations are not able to accomplish isolation or containment
7. Organizations are facing increased regulatory pressures for ICS/SCADA

Finally, compliance has become a growing concern for those managing OT systems. Seven in ten report mounting compliance pressures over the past year, and 78% feel this trend will continue for the next two years. According to the report, the regulations making the most significant impact are:

1. The EU Data Protection Directive (GDPR)
2. International Society (ISA) Standards
3. The Federal Information Security Management Act (FISMA)

Partners Matter

One source of risk associated with IT-OT is the added exposure of infrastructure to business partners. Granting appropriate privileged access to the appropriate personnel is critically important. The Fortinet/Forrester Research study found those organizations that were most successful with securing their environments were also 129% more likely to severely limit or even deny access to their business partners.

Similarly, they were also more careful about allowing access to IT providers, granting only moderate access. Finally, these top-tier organizations were 45% more likely to keep certain security functions in-house rather than outsourcing them. However, they are also more likely to have outsourced network analysis and visibility.

So, what does this all mean? Partners – and the types of relationships that organizations form with them – are meaningful. Granting the appropriate access, making the best outsourcing decisions, and identifying situationally-ready partners will be vital to securing OT systems amid digital transformation.

As industrial systems continue to evolve, OT and cybersecurity leaders are faced with new challenges that have led to new priorities. Due to the complexity of IT/OT convergence, organizations have been deliberate in their adoption of processes to avoid data leakage or other modern threats. To appropriately protect their high-value cyber-physical assets, those who manage and maintain critical infrastructure must keep abreast of the latest security trends, especially those related to IT/OT convergence, and understand how to secure their migration into this broader, digitally transformed landscape. ■

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

Are You Ready To Move SAP To AWS?

Best practices for an effortless fast move of SAP applications to AWS

By Santosh Prasad, Awaiz Usman, Chetan Ramachandra and Hemant Poddar

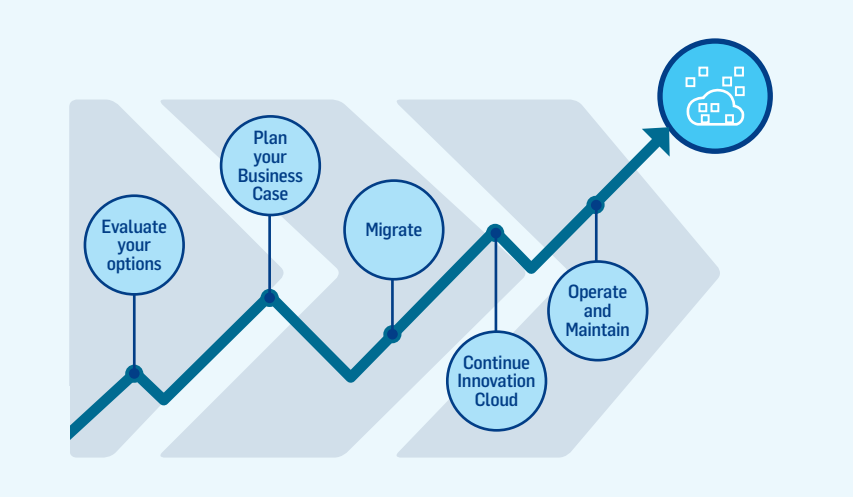
Cloud migration is considered challenging by more than 60% of IT decision makers. However, cloud is fast becoming the new normal. The move to the cloud has two major workstreams: migration of enterprise workloads and modernization of existing applications. The biggest challenge faced by most organizations is managing the complexity of these processes— individually and in parallel—with resiliency and security.

Many SAP customers have been running SAP on-premises for decades and have been reluctant to harness the benefits of the public cloud. But as the public cloud has transformed IT and businesses, on-premises hosting has become harder to justify. While the traditional benefits of the cloud — superior scalability and lower costs — have only become more apparent as the technology has matured, SAP on public cloud has also overtaken on-premises hosting in areas like security, historically used to justify staying on-site.

SAP Migration Roadmap

Migrating your data and applications to cloud is a multi-step process that requires a lot of time and attention to successfully complete the task. An organization needs the proper strategy and mindset to go through the migration smoothly. Careful planning and point-by-point consultations are crucial for the move to the cloud to be successful.

Before beginning any migration, it is important to understand what you're moving and why. Your overarching cloud migration strategy should be based on how many applications you intend to move: Are you moving a single application or shared resource, such as a database or mail server?, A cluster of related applications?, Your entire portfolio?



Cloud Migration Roadmap

If your applications have been built with the cloud in mind, then they are a short pit-stop on your cloud migration journey. Even for the application that were not built with cloud in mind, consider low criticality and low impact applications for immediate migration.

For complex migrations, a carefully planned cloud migration strategy is your path to successfully moving legacy applications to the cloud without breaking your workflows.

Our recommendations for complex migration:

Service-first cloud migration

Migrating all the services for your application portfolio before moving the application helps ensure that all dependencies are met and any application you migrate to the cloud will function as expected.

Adopt a hybrid approach

Migrating to the cloud does not have to be an all-or-nothing proposition. You can incorporate your existing systems and applications into a hybrid cloud. This approach lets you start capitalizing on cloud capabilities while continuing to make the most of your existing investments in on-premisess environments.

Replace old with new

Consider replacing your legacy applications with an existing software-as-a-service (SaaS) solution. A made-for-cloud version of your application can be an effective shortcut with a higher initial cost and lower deployment effort.

Start from scratch

Redesign your application with microservices to simplify your cloud migration. This process can cause some initial disruption and require resource commitment. But it often pays off with a state-of-the-art application that takes full advantage of the cloud.

The significant drivers for cloud migration are:

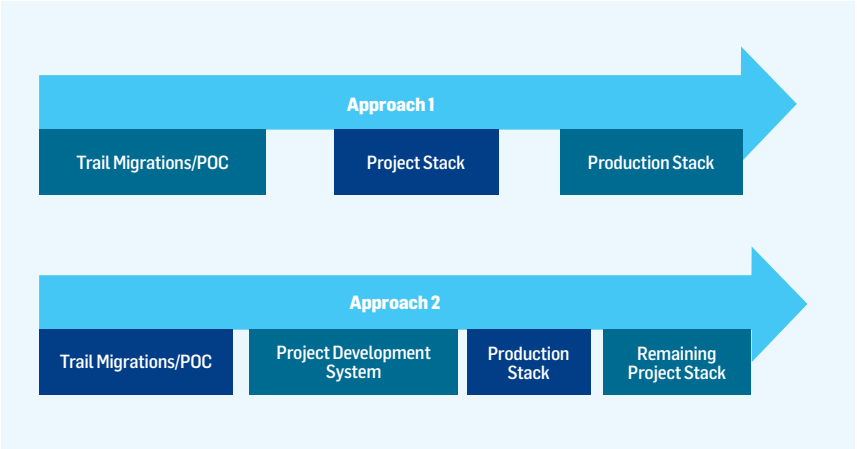
- Infrastructure end of service life
- Business driven upgrade requiring re-platforming (for example, ECC to S/4 Hana)
- On-premises capacity bust
- Data center exit to support cloud transformation programs

Following are the specific considerations while moving SAP applications to cloud:

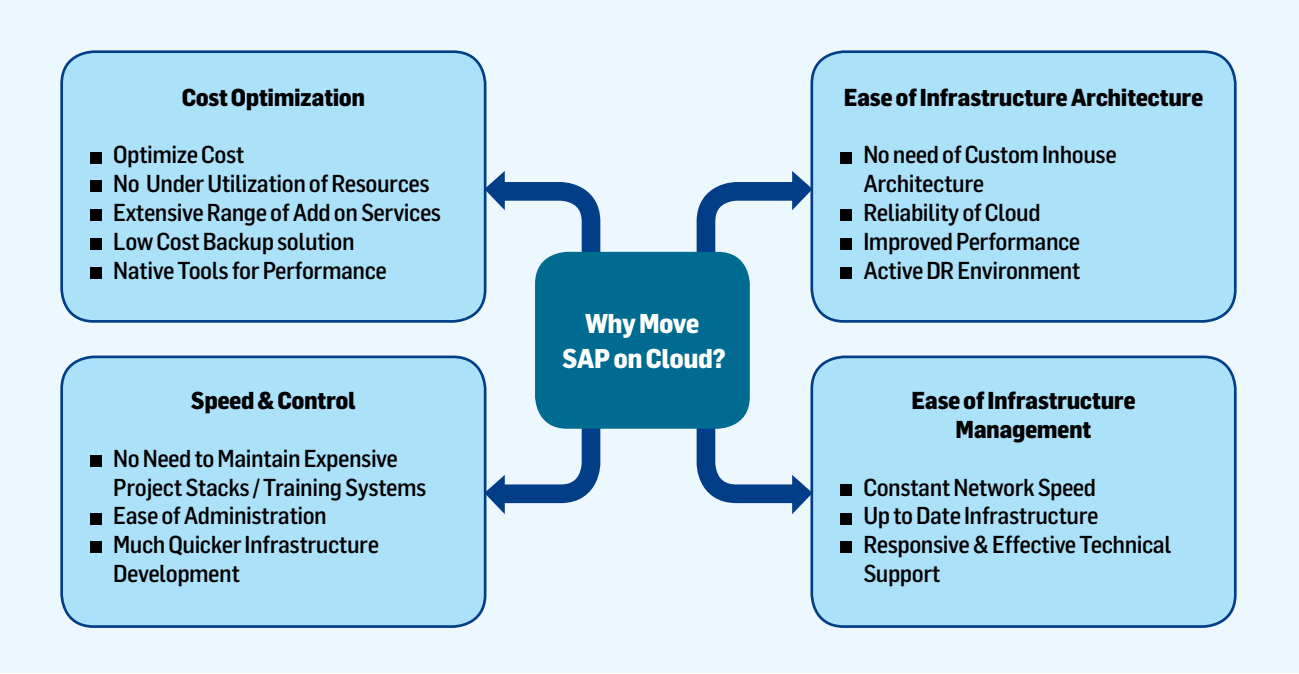
- Move smaller, less critical SAP systems to cloud first
- Several trail migrations to be done until desirable runtime is achieved consistently. This allows you to adjust the number of R3 load processes required for the migration and adjust the sequence of table exports
- In addition to the time to export/import/migrate the database, the time it takes to ramp down and ramp up the interfaces must be taken into consideration. This must be tested end-to-end during dress-rehearsal or pre-production migration

A typical SAP cloud migration project could run for months depending on the complexity of the project. A straightforward "life and shift" SAP migration could be achieved much quicker compared to a complex migration requiring an upgraded SAP solution on target.

The duration of the migration mainly depends on the size of the database. SAP migrations combined with upgrades and unicode conversions will take longer. However, depending on the use case, there are several tools in the market to complete any complex SAP migration typically over a weekend.



Cloud Migration Approaches



Migration Benefits

Migration projects involving system conversion, for example SAP ECC to S/4 HANA will require a comprehensive testing strategy and end user training. The 'lift and shift' projects will also require some level of testing to be performed especially around custom programs and interfaces.

Broadly speaking, the following categories exist:

- SAP Basis/Infrastructure testing covering basic aspects of infrastructure like security scans or penetration tests, High Availability/Disaster Recovery scenarios, alerting and validating shutdown/startup procedures, etc.
- Functional/ABAP testing covering User Acceptance Test, Regression Testing & Integration testing involving key interfaces
- Performance testing that will simulate production like load (users, batch jobs) on a production sized test system. This can also include testing the performance of critical interfaces

Benefits post Migration

There are many problems that can be solved by moving to the cloud. Some of the typical scenarios that will benefit from cloud migration are mentioned as below:

- Minimal CAPEX costs – buy what you need and pay for what you use
- Ease of administration – more control over infrastructure
- Time to deploy infrastructure (compute, storage, networking) is much quicker than on-premisess (few minutes vs few months)
- No need of custom in-house Architectures, use standard AWS Architectures
- AWS Technical Support – responsive and effective
- Reliability of AWS – multiple availability zones, guaranteed SLA's
- No underutilization of resources - Scale up and Scale down when needed and quickly
- Hardware specs of AWS servers are higher, hence better performance (average response times)
- When a server reaches EOSL, a pop up is displayed, just shut down/start-up will migrate VM to new hardware, so customers are not using old routers or outdated equipment
- AWS providers schedulers to shutdown/start servers based on a schedule. Non-prod SAP systems are shutdown during non-business hours that results in cost savings.
- Extensive range of services like S3, cold storage, etc. S3 is used to store backups vs using expensive tape solutions on-premisess

Conclusion

Cloud adoption is inevitable in this virtually equidistant world of technology. Your organization will have to move to the cloud sooner than later. But it's crucial to comprehend why you are adopting cloud solution in the first place! While it may seem obvious, however going through a set of proven steps and best practices is essential to attain your desired results. It is highly advisable to clearly outline your motive for move to cloud to keep your cloud journey on track and to prioritize among the key drivers. ■

Santosh Prasad is Partner & Service Line Leader, Cloud Application Management Services (Cloud Move & Build), IBM; Chetan Ramachandra is Managing Consultant & Cloud Architect, IBM; Hemant Poddar is Delivery Project Executive, Complex Projects, IBM India; Awaiz Usman is Managing Consultant & SAP Technical Architect, IBM UK

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

facebook.com/digitgeek

digit.in/facebook

4 Technology Trends That Will Mark The New Normal

One caution: forecasts in this rapidly changing environment are just a broad indicator, but it is a good place to start

By Dipanjan Mitra

It took some time but by now, most of us have accepted the new reality, that is, living life with COVID-19. This year's pandemic has brought the entire world to a standstill and forced organizations to alter their business plans, infrastructure and working pattern. By now, most of us are working from home (WFH).

It is to the credit of the IT managers that they managed to save the businesses—and thus the broader economy—by enabling the shift to remote working mode. But as we prepare for a prolonged period of this arrangement—or a slightly diluted form of it—there are questions that need to be answered. What works in distress situations is not the best thing to go for in normal situations, new normal, as we call it now. Three things must be kept in mind, when we talk of the new normal.

- No one knows what it will be, as things are still uncertain. It is a moving target and what is forecast, prophesized or plain speculated are based on what is known now. It is largely an extrapolation of the present at best and blind-men-and-elephant story at the worst.
- One thing is for sure. It will not be same as the situation before the pandemic.
- It will also not be the same as what we have seen in the lockdown.

Still, we have to start somewhere. We sift through some of the recent research to find a broad direction.

Here are some trends.

Security as the single-most important thrust

WFH cyber habits, such as password re-use and letting family members use corporate devices – lead to putting critical business systems and sensitive data at risk remains.

Losing control of corporate devices is a real concern and this is highlighted in a CyberArk survey, which says 77% of remote employees are using unmanaged, insecure "BYOD" devices to access corporate systems.

Cybercriminals have also increased their activity with more and more people WFH now. Add to that, the lacklustre handling of corporate devices and data, as highlighted by a Check Point Research survey, which says over 75% of respondents saying their biggest concern was an increase in cyber-attacks, especially phishing and social engineering exploits; 51% saying that attacks on unmanaged home endpoints were a concern, followed by attacks against employee mobile devices (33%). Add to that, just 29% deploy endpoint security on employees' home PCs and only 35% run compliance checks. 42% say their company invests in cyber-security training. This highlights how exposed organizations are to fast-moving, 5th generation cyber-attacks that target remote workers.

This is not to say organizations are completely ignorant about cybersecurity or do not have specific policies in place. However, in the current scenario, they lack the adequate security guidelines necessary for secure remote work. A OneLogin study

proves this as is reflected in its survey, which shows 30% of employees surveyed admitting to having an online account compromised during remote working, with 10% of these failing to change their password afterwards.

Cloud Acceleration

As more and more organizations try to adjust to the sudden shift to remote working and accept the New Normal, moving workloads to Cloud seem the popular choice for organizations.

As a MariaDB survey reveals, organizations are setting up remote access for all employees (57%) and moving more applications to the cloud (51%).

However, with more and more organizations embracing the Cloud and even increasing their Cloud investments, some skepticism remains with regards to trust. How well can you trust your public cloud provider?

A Yellowbrick Data's survey shows that more than a quarter (27%) of enterprise leaders saying they do not trust public cloud providers to prioritize their business needs. With the above statistic in mind, it is not surprising that risk mitigation remains a critical consideration, with 82% of respondents saying they want hybrid or multi-cloud options to spread any risk from their cloud investments, along with an additional 67% saying there are some parts of their business they will not trust to any single cloud vendor.

A key point to note here is organizations also need to ensure their data is protected in the Cloud. Otherwise, what is the difference between legacy systems which are weak and vulnerable to attacks and advanced Cloud protection systems? A Veeam Software study points out that many organizations (40%) still rely on legacy systems to protect their data without fully appreciating the negative impact this can have on their business. The vast majority (95%) of organizations suffer unexpected outages and on average, an outage lasts 117 minutes (almost two hours). Hence, Data storage, protection and backup are crucial to a successful and secure Cloud adoption.

End-user Technology Coming to the Forefront

COVID-19 pandemic, leading employees to WFH, has been a blessing in disguise not only for Cloud-based technology solution providers but also for organizations trying to figure out ways to 'keep the lights on'. Cloud-based offerings like Zoom, Slack, and Microsoft Teams, and other remote learning tools are increasingly being used for office collaboration amongst businesses and remote education and training amongst educational institutions. Public cloud providers like AWS, Google, Microsoft and Salesforce are providing products-as-a-service to empower companies with increased computation and storage capabilities at a relatively low investment. For instance, Nutanix announced an enhanced free trial of its Frame Desktop as a Service (DaaS) for enterprises in the APAC region in February 2020 to enable remote working for enterprises amidst the COVID-19 outbreak. Infact, a GlobalData study outlines that the COVID-19 pandemic has accelerated the demand for digital technologies to ensure resilient enterprise business operations. Subsequently, a surge in demand across the Asia-Pacific (APAC) region has resulted in cloud-based offerings outshining traditional products.

Moreover, there is a high demand for Software-as-a-service (SaaS) based offerings from enterprises, specifically for teleworking and remote conferencing.

Agile Adoption and Continuous Intelligence

Organizations are upping agile adoption for increased benefits during the pandemic. Agile adoption improves key capabilities needed to respond to current business challenges, especially those resulting from the pandemic. This is supported by a Digitalai's survey, which reveals 60% of IT and business professionals saying Agile has helped increase speed to market, 41% agreeing they are better able to manage distributed teams, and 58% saying they have improved team productivity. Therefore, it is clear these practices are invaluable during these challenging times.

There is also an increasing demand for a new category of software called Continuous Intelligence among C-level executives. Key industry trends — including accelerated cloud migration, the rising importance of rapid data insights, and the emergence of DevSecOps — are converging to drive huge demand for continuous intelligence. Continuous Intelligence allows organizations to more rapidly deliver reliable applications and digital services, protect against modern security threats, and consistently optimize their business processes in real time. This empowers employees across all lines of business, development, IT, and security teams with the data and insights needed to address the technology and collaboration challenges required for modern business. As per a Sumo Logic survey, in today's ever-changing business landscape, those businesses that operate using a software-driven model will be the most successful. These businesses recognize the power of transforming enormous volumes of data generated by digital operations into real-time insights that propel further success. The ability to do this in real-time, all the time, across multiple functional disciplines, lies at the heart of Continuous Intelligence.

In this New Normal, organizations need to foster a culture of cyber resilience, focus on protecting critical capabilities and services and keep all business response and continuity plans updated. As a World Economic Forum (WEF) report indicates, by following cyber resiliency, organizations will be able to successfully shape a responsible course of action that balances short-term goals against medium- to longer-term imperatives. Agile adoption and Continuous Intelligence can also help in this new era. ■

TRANSFORMATION
A Sectoral View

How industry value chains can be positively impacted by digital transformation initiatives, especially leveraging big data, IoT and AI

By Saumya Chaki

PART III: ▸RETAIL ▸HOSPITALITY

The author is Data Platform Solutions Lead at the Services Integration Hub in IBM and has written three books

RETAIL

Disrupting Retail – With Intelligent Data

The rise of customer led disruption is not new to the retail industry, however, what is truly transformative is the need for retailers to focus on the digital value chain

Retail industry has been on the cusp of a silent revolution, shifting from a product centric model to a customer centric model. Disruptions in technology like the internet in the 1990s, mobile in the 2000s and digital technologies in the last 5-6 years have resulted in a technology savvy customer, who has a very different set of expectations from a product centric world of retail, where the retailer would procure products at optimal prices and sell to customer at higher prices.

The rise of customer led disruption is not new to the industry, however, what is truly transformative is the need for retailers to focus on the digital value chain – one focused on collecting data from multiple sources (products, customers and locations), analyzing the data to generate insights and using the insights to trigger actions. Amazon Go is an Amazon initiative of convenience stores, where customers can choose and buy items without having to go to a till or a self-checkout station. The store is fitted with cameras and sensors and tracks every shopper's behavior in the store, the data collected is used to generate insights and trigger actions on making the shopping experience better. The digital value chain can be applied across the retail value chain as we shall examine in the next section.

Transforming Retail with Data

At the cusp of digital disruption in retail is 'data' that is helping retailers move from a product centric view to a customer centric view. Let us review the value chain of a retail enterprise to visualize the disruptions that digital technologies are bringing at each stage.

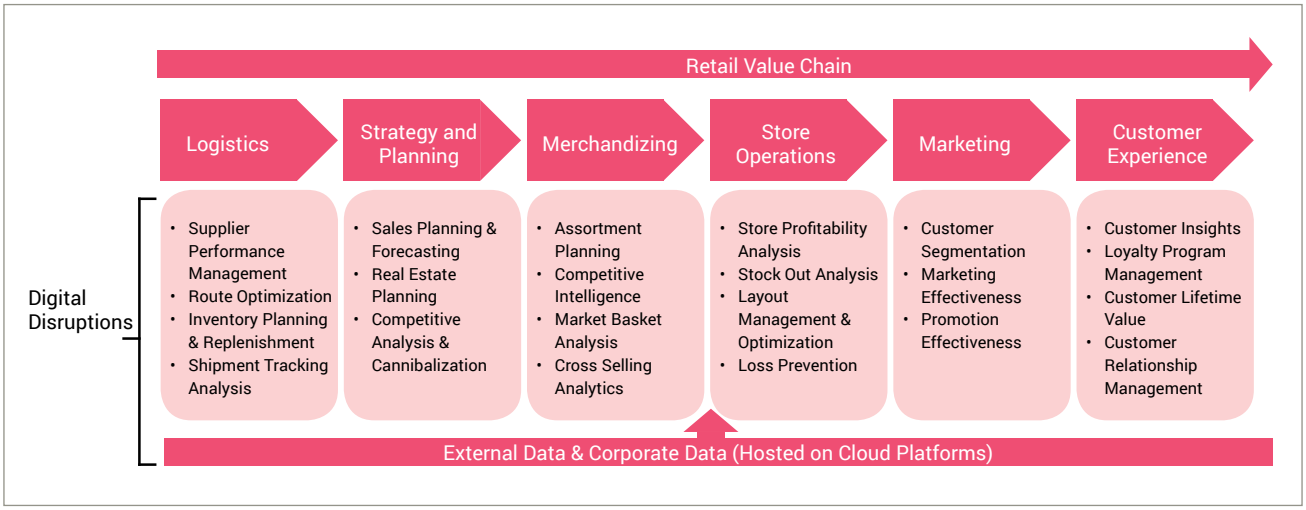
- **Logistics** – Logistics is a key challenge in a retail business irrespective of brick and mortar or online. At the core of the logistics are suppliers who ship their goods either to the physical store or to customers in case of online shopping. Supplier performance is a key enabler of retail businesses. Other key

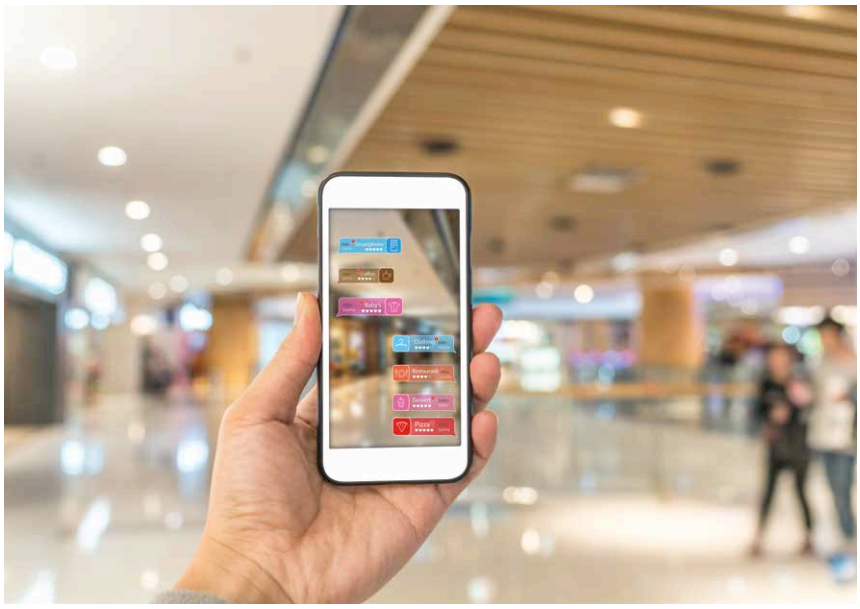
areas where big data analytics and artificial intelligence can be applied are in route optimization, inventory planning and replenishment and shipment tracking. In route optimization digital data sets like weather data, traffic data can be used to apply insights in route planning, resulting in optimized logistics. IoT sensors can be used in warehouses and stores to determine inventory levels and potential stock outs on fast moving items that can be fed into inventory management and replenishment algorithms.

- **Strategy and Planning** – Retailers need to perform sales planning & forecasting based on analysis of sales across channels and forecast demand. Use of PoS data in analyzing sales as well as forecasting based on advanced analytical models can help plan JIT inventory. In addition, stores need to be located strategically to earn customer mindshare, thereby real estate planning becomes a key planning driver. Retailers also need to analyze the impact of brands on competing brands by analyzing competitive sales data from 3rd party providers integrated with big data technologies.
- **Merchandizing** – One of the key differentiators in retail industry is the ability to gather competitive intelligence on product/brand trends, customer preferences in the target group. In addition, market basket analysis across channels provide retailers deep insight into customer behavior and buying trends. IoT, big data analytics and mobile are the enabling technologies that provide significant value. Assortment planning leverages the insights from market basket analysis and competitive intelligence, enabling retailers to focus on the right items to stock, in the right quantity at the right moment in time. Based on customer buying trends and social media analytics, retailers can also look for potential cross sell opportunities.
- **Store Operations** – With increasing pressure on margins and lower costs associated with online shopping, retailers need to analyze store profitability proactively. Near real time insights from store systems into data lakes, provide valuable insights about store performance including stock out analysis, loss analysis. Insights around customer behavior based on layout management helps retailers organize their store layout and placements better.
- **Marketing** – One of the key drivers of digital disrupting is around making marketing more efficient and fleeter footed. Customer segmentation analysis based on current data and aspirations, helps plan promotions better and feed into marketing effectiveness measured through targeted Promotions. Learnings from these initiatives are continuously fed into CRM systems to enhance the customer experience and enhance marketing effectiveness.
- **Customer Experience** – At the core of this new customer centric model that retailers have adopted, is the customer experience. Traditionally retailers have used customer loyalty programs, which are now enhanced by customer insights and understanding the value of the relationship through customer lifetime value. These insights are leveraged by CRM systems and processes to plan promotions and offers. With the customer increasingly tech savvy and spoilt for choice, retailers are now pushed to be ahead of the game when it comes to customer service.

The key disrupting technologies that are reshaping the way retailers are making the transition to a customer centric business are as follows:

- **Mobile** – Mobile displays and workstations that help customers view product catalog in availability in store as well as pay through payment systems, enhances the customer experience in stores such as Argos.
- **IoT** – IoT sensors in store to pick up customer movements, 3D printing for custom products and parts.
- **Artificial Intelligence and Big Data** – AI and big data are crucial





Importance of digital technologies in providing a seamless customer experience is key to customer engagement

differentiators for retailers aiming to build a consolidated view of customer preferences and enhance the customer experience across channels of interaction.

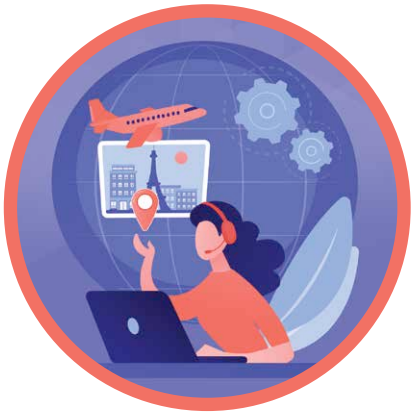
- **Smart Beacons** – Smart beacons work with Bluetooth technology to alert retailers, when customers are near the store or signage and help them provide customized offers at a given time. This takes targeted Marketing to a new level. Retailers like Target, Walgreens have already rolled out new beacon deployments.
- **Virtual Reality** – Customers prefer to hold, touch while buying certain items like clothes, cars or homes. Virtual reality and augmented reality are empowering customers to experience the product without being near it and may enable them to take buying decisions.

As is evident from the transformational impact of digital technologies at each stage of the retail value chain, companies are increasingly looking at leveraging these technologies not only for productivity enhancements, cost optimization but also as a differentiator in enhancing revenues through enhanced customer experience and targeted campaigns. The key benefits that digital disruption has provided the Retail industry are as follows –

- **Seamless Omni-Channel Experience** – Ability to ingest data from across the supply chain and in stores, provides retailers the ability to leverage the insights that helps provide a seamless omni channel experience to customers. This is at the core of the customer centric strategy that retailers are moving to.
- **Cost Optimization** – Digital technologies have helped optimize the cost of operations by analyzing data across the supply chain which can be analyzed to generate insights across logistics, merchandizing, store operations and marketing.
- **Customer Retention** – Armed with the digital technologies and enhanced customer service capabilities, retailers are better placed to handle customer churn as well as acquire new customers. However, customer loyalty can be earned by continuous innovation in optimizing the supply chain as well as enhancing the customer experience.
- **Productivity** – As we have seen right across the value chain digital technologies have brought significant productivity gains through automation, big data analytics and IoT. Ability to handle and process unstructured data in form social media sentiment analysis, weather data for route planning optimization has also enhanced productivity of enterprises which would spend many man hours analyzing such data sets and generating insights.
- **Revenue Models** – With customer centricity at its focus, retailers will look to create customized offers/ product bundles to meet customer buying behavior. This creates an ability to generate new revenue streams as well as look at cross sell opportunities based on market basket analysis and competitive intelligence. The ability to merge multiple data sets and generate insights creates new revenue generating models and opportunities.

Importance of digital technologies in providing a seamless customer experience is the key to engaging with customers today.

According to the *PwC Future of Customer Survey Experience Survey of 2017-18,* the three things customers were ready to pay more for were – convenience, speed & efficiency and friendly & welcoming service. Interestingly 96% of survey respondents mentioned they wouldn't interact with a company providing unsatisfactory customer experience ■



HOSPITALITY

Transforming The Hospitality Sector With Digital Technologies

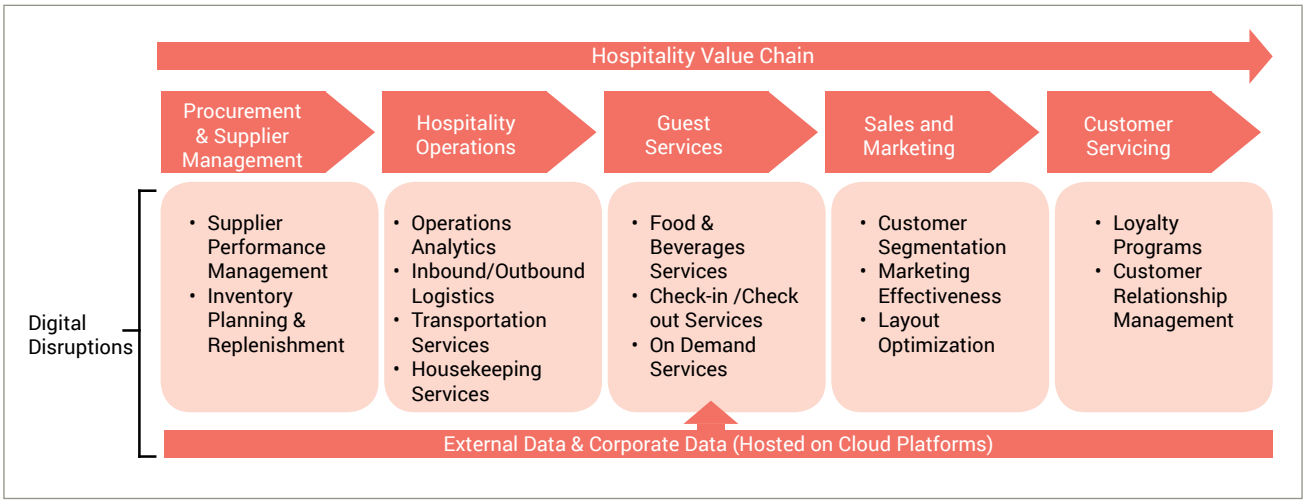
The disruption that digital technologies bring to a hospitality provider can be a differentiator in the globally competitive business

One of the industries that are in a state of disruption has been the travel and hospitality industry. At the core of this disruption are themes of mobility, flexibility and easy availability of information that help customers make informed choices. Gone are the days where travel meant visiting a travel agent for booking tickets or getting a good hotel deal. Aggregators like Airbnb and Skyscanner are adding to the disruption by providing customers with price comparisons and features that help them take informed decisions around their travel preferences and choices.

At the epicenter of this disruption are a set of digital technologies including Big Data Analytics, Mobile Apps, Internet of Things (IoT) and Artificial Intelligence (AI) which are helping hospitality providers reinvent themselves and provide a rich hospitality experience to customers.

Transforming the Hospitality Sector with Digital Technologies

At the cusp of digital disruption in the hospitality sector is 'the insights from data' generated at each stage of the value chain, that is empowering hotels and their partners to transform their business models. Let us examine the



value chain and how digital transformation is a differentiator at each stage of the value chain.

- **Procurement and Supplier Management** – Hospitality providers are dependent on procurement of goods and services to manage the properties. Examples of procurement could be furniture, soaps, towels, smart devices, security services, etc. Use of IoT devices and Big Data Analytics for managing the procurement processes efficiently as well as manage inventory. Supplier Performance analytics help hospitality providers gauge the performance of suppliers over time and identity potential areas of improvement.
- **Operations** – Hospitality industry runs on narrow profit margins resulting in a need for streamlined and optimized operations. The key aspects of operations of a hospitality provider include housekeeping services, transportation services for guests and in-bound logistics around procurement of goods to run the operations. Data from operations is collected in near real-time through IoT sensors, operational systems and Big Data Analytics leveraged to perform Operations Analytics to ascertain the efficiency of end-to-end operations. Use of mobile housekeeping apps helps in keeping the staff aware of inventory which can be used as a feedback into the sourcing processes. The impact of planned events like conferences and disease outbreaks like the Coronavirus are also factored into the operations planning.
- **Guest Services** – At the core of any hospitality business is the customer. Guest services are the key differentiator for hospitality providers and include Food and Beverages services (bars, restaurants, room service, etc.), Check-in/ Check-out services (use of mobile apps as part of check-in services wherein electronic key cards for room access are provided to the customer's mobile device; digital housekeeping apps can update the reception that a room is vacant and ready to check-in; check-out can trigger notifications to the transport desk in case a guest needs to be dropped to the airport), On-demand services (like doctor, physical training, room heating controls based on IoT sensors. etc.). Hotels like Marriott are leveraging AI-based chat bots to help customers make changes to reservations or check on status of redemption vouchers.
- **Sales and Marketing** – Hospitality providers are increasingly driven by customer demands and preferences and are going all out to collect data around Customer Segmentation and Marketing Effectiveness of campaigns. Customer Segmentation helps understand customer demand based on buying behavior (room type, nature of guest services used, wish list, etc.) thereby creating opportunities for customized marketing campaigns.
- **Customer Servicing** – For hospitality providers to succeed in an increasingly competitive market, they must serve customers well through the end-to-end life cycle. Customer Loyalty programs need to integrate
data from multiple channels to provide a 360-degree view of customer preferences and design loyalty programs to meet the changing needs. The CRM process and systems need to provide inputs to the Customer Loyalty program to ensure effectiveness of campaigns and provide relevant offers.

The key disrupting technologies that are reshaping the way hospitality providers are making the transition to a digitally-savvy enterprise are as follows:

- **IoT** – Use of IoT sensors to help control room temperature and capture customer preferences. IoT data can be leveraged to analyze when the customer visits a property and integrated with marketing campaigns to send out offers during a preferred season of travel.
- **AI and Big Data** – AI and Big Data are crucial differentiators for hospitality by ingesting data from across the value chain that help optimize

With customer centricity at its focus, hospitality providers will look to create customized offers to meet customer-buying behavior. This creates an ability to generate new revenue streams

processes and operational costs. Real-time insights about inventory help hotels plan their procurement cycles better. Use of AI chat bots in guest reservation and e-concierge is helping make the customer experience better and providing these services 24*7.

- **Mobile Apps** – Hospitality providers are creating a new customer experience by providing guests with facilities like mobile check-in, ordering room services though mobile apps and electronic key cards sent to mobile phones for unlocking room doors. Mobile apps could also provide services like food and beverage bills and making reservations/cancellations.
- **Virtual Reality** – Virtual Reality is being leveraged by hotels in providing customers a virtual tour of the hotel to help customers understand the layout and services on offer. Interactive maps are provided in rooms to help customers explore the hotel layout and surroundings.

As is evident from the transformational impact of digital technologies at each stage of the hospitality value chain, companies are increasingly looking at leveraging these technologies not only for optimized operations and cost optimization but also as a differentiator in enhancing revenues through enhanced customer experience and targeted campaigns. The key benefits that digital disruption has provided are as follows:

- **Cost Optimization** – Digital technologies have helped optimize the cost of operations by analyzing data integrated across the hospitality chain which can be analyzed to generate insights across Procurements, Operations, Guest Services, Sales and Marketing and Customer Servicing.
- **Customer Retention** – Armed with digital technologies and enhanced customer service capabilities, hospitality providers are better placed to handle customer churn as well as acquire new customers by understanding customer preferences better. However, customer loyalty can be earned by continuous innovation in optimizing the value chain as well as enhancing the customer experience.
- **Reputation** – Success in the hospitality industry is greatly driven by customer experience and feedback. Customers post reviews in travel websites like Trip Advisor and on social media sites like Facebook and Twitter. Hospitality providers not only promote themselves on social media by having their own pages/promotions but also need to learn from the feedback provided about their properties and guest experience. Social media data can provide unique insights about customer satisfactions and needs.
- **Revenue Models** – With customer centricity at its focus, hospitality providers will look to create customized offers to meet customer-buying behavior. This creates an ability to generate new revenue streams as well as look at cross-selling opportunities-based on customer segmentation and competitive intelligence. The ability to merge multiple data sets and generate insights creates new revenue generating models and opportunities.

The global hotel industry had revenues of over USD 600 billion in 2018 and is growing at 6-7% annually. The disruption that digital technologies bring to a hospitality provider can be a differentiator in this globally competitive business. Customers are well informed with access to information and hospitality providers are leveraging digital technologies to engage better with customers. Some hotels like Marriott in China are exploring facial recognition technology for enhancing security and privacy ■

Double Scoop

Two times the revelation

Sachin Gavankar

Head - IT, EsselWorld Leisure

MY FAVORITE SPORTSPERSON

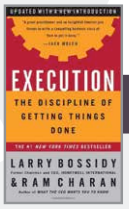
Sachin Tendulkar

MY PEER IN THE IT COMMUNITY

Ketan Shende,
Sr. GM - IT,
Cummins India

MY FAVORITE ACTIVITY IN THE COVID ERA

Painting



A BOOK I LOVE READING

Execution: The Discipline of Getting Things Done by Larry Bossidy & Ram Charan

MY TECH IDOL

Charudatta Naik

A CUISINE I LIKE THE MOST

Malvani Fish Curry

Ketan Shende

Sr. GM - IT, Cummins India

A VIDEO CONFERENCING PLATFORM I USE THE MOST

Zoom

MY FAVORITE AUTHOR

PL Deshpande

MY FAVORITE SINGER

Lata Mangeshkar

A PLACE I'D LIKE TO VISIT IN THE NEAR FUTURE

Rajasthan

MY FAVORITE COLOR

Navy Blue

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

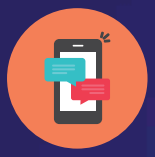
digit SQUAD

Here is your chance to become a Digit certified tech influencer

Benefits of Digit Squad Member

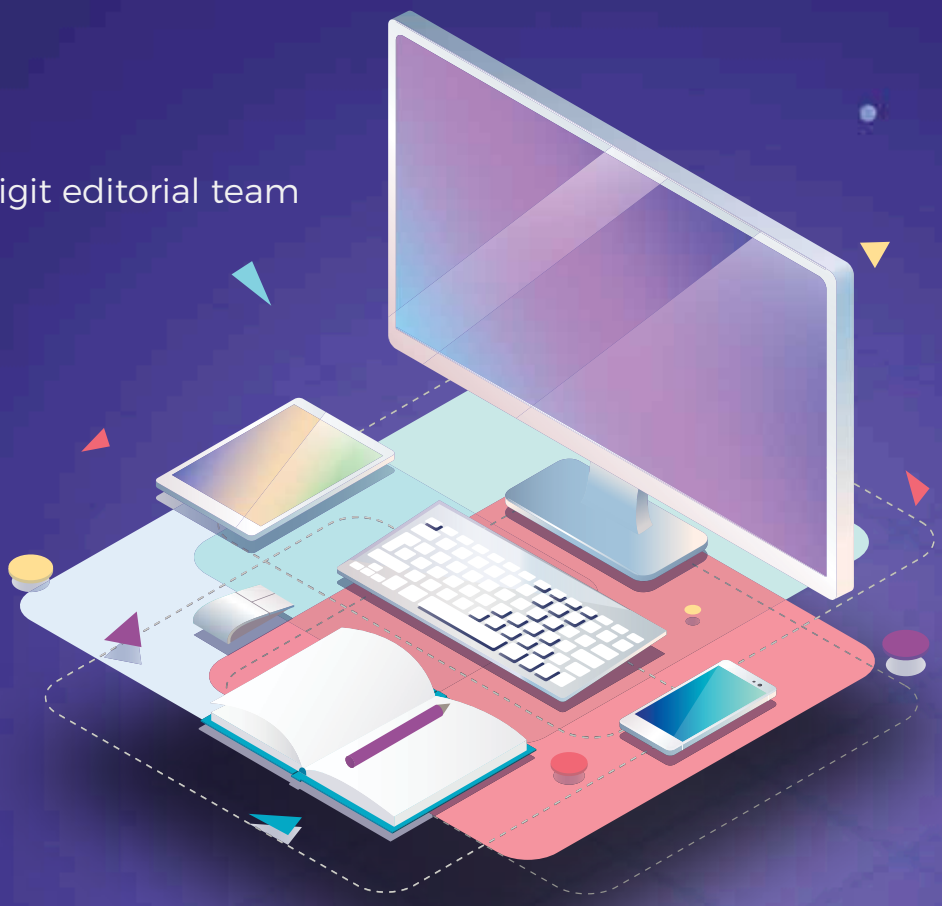
Launch your own tech channel on Digit.in

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