Opinion | Pg 12
Facebook Crisis And Network Security In India

Insight | Pg 18
State of Martech 2018

IT NEXT

FOR THE NEXT GENERATION OF CIOs

THE 2018 CISO SURVEY

Integration & Compliance Top Challenges for CISOs

6 out of 10 security leaders report outside the IT department

July 2018 | ₹100 | Volume 09 | Issue 02 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

PAHWA™ GROUP
Innovation is life

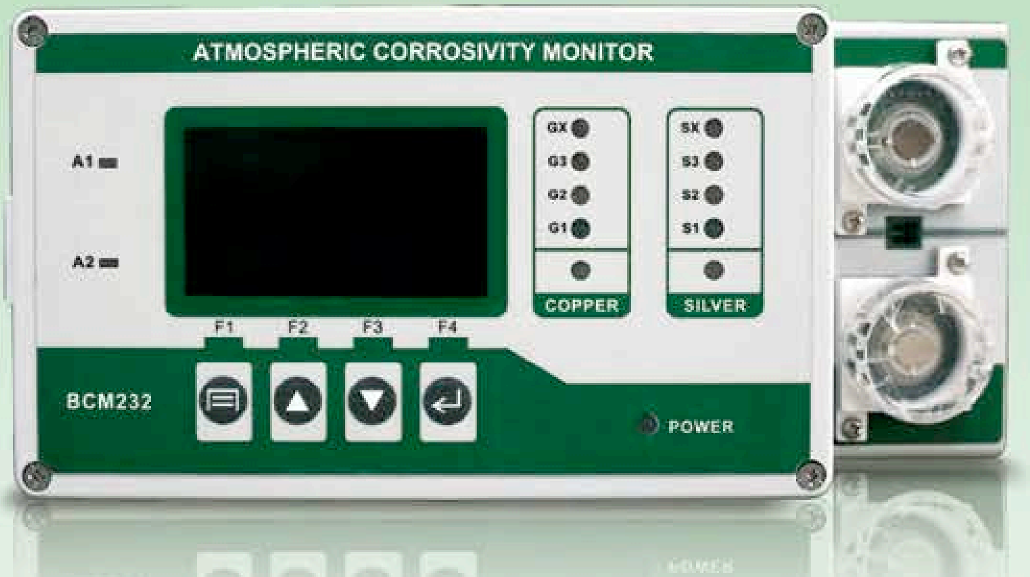
PREVENTION

is more economical than cure

Corrosion due to gaseous contaminants in the environment in data centers, server rooms, control / DCS / switchgear rooms leads to sudden failure of entire operations, and consequent high replacement cost.

Bry-Air®

Atmospheric Corrosivity Monitor (ACM)



Backed by
Brycare™ Service

**Measures and rates corrosivity potential of indoor air.
Enables you to take timely action, before the damage happens.**

Vulnerable industries:

- Paper Pulp
- Chemicals & Fertilizer
- Iron & Steel
- Petrochemicals & Refineries
- Power Generation
- Textiles
- Data Center / Server Room
- Banking and Financial
- Telecom
- Media and Broadcasting
- BPO / KPO / ITES
- Hospitals
- Aviation (Airports)

World leaders in Gas Phase Filtration Systems

BRY-AIR (ASIA) PVT. LTD.

www.bryair.com

419-420, Udyog Vihar, Phase-III, Dist. Gurugram 122016, Haryana, India
Phone: +91-124-4184444 • E-mail: bryairmarketing@pahwa.com

Delhi • Chandigarh • Mumbai • Pune • Vadodara
Kolkata • Bengaluru • Hyderabad • Chennai • Kochi

RB/BA/1821FCA1

Which security path do you want to choose?

> While the CISOs may complain about too much of compliance related work, it is those compliance requirements that help them achieve what they want to. The regulators assume the role of the bad guy.
>
> **Shyamanuja Das**

That integration of multiple security solutions and compliance have emerged as the top two challenges in our security survey should come as not much of a surprise to those tuned in. But even to the practitioners it may look a little surprising that six out of ten security leaders now report outside of IT organization.

A small part of that—like banking and insurance—may be driven by specific mandate from the sectoral regulators but the logic that prompts these regulators to go for such specification applies to others too. There's an inherent conflict of interest between business-aligned IT which wants to do things faster and the risk-aligned security that wants to ensure that everything is in place.

While the CISOs may complain about too much of compliance related work, it is those compliance requirements that help them achieve what they want to. The regulators assume the role of the bad guy.

However, as many of the organizations have figured out, it is probably apt to divide the security roles into two – one operational IT security and one risk-based cyber security. I call it bi-modal security. Here, one set of security professionals ensures that what needs to be protected is protected in the best manner possible, while the other set is continuously scanning for new threats, new challenges and are even willing to take on the attackers in a combative role. Needless to say, the two sets of people need to be part of two teams. The first is essentially an extension of IT; the second could be part of Risk.

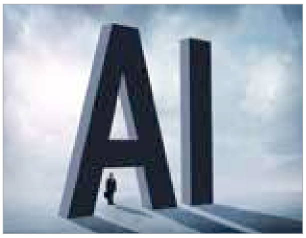
While the line between the two may not be as sharp in many organizations, informally, the roles are already getting separated.

As a security professional, you need to decide what track you want to pursue and acquire skills accordingly. More about this later.

Enjoy the survey findings.

JULY 2018
VOLUME 09 | ISSUE 02

Content



Cover Design:
CHARU DWIVEDI

ADVERTISER INDEX

Bry Air Asia	IFC
Vodafone	BC

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

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

EDITORIAL
Managing Editor: Shyamanuja Das
Content Executive-Enterprise Technology: Dipanjan Mitra

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

SALES & MARKETING
Director-Community Engagement: Mahantesh Godi (+91 9880436623)
Brand Head: Vandana Chauhan (+91 99589 84581)
Assistant Product Manager-Digital: Manan Mushtaq
Community Manager-B2B Tech: Megha Bhardwaj
Community Manager-B2B Tech: Renuka Deopa
Associate-Enterprise Technology: Abhishek Jain

Regional Sales Managers
South: BN Raghavendra (+91 9845381683)
North: Deepak Sharma (+91 9811791110)
West: Prashant Amin (+91 9820575282)

Ad co-ordination/Scheduling: Kishan Singh

Manager - Events: Naveen Kumar
Manager - Events: Himanshu Kumar

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

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

THE 2018 CISO SURVEY

Integration & Compliance top challenges for CISOs

Integration of multiple solutions and compliance are identified as the top two challenges by the security leaders.

By Shyamanuja Das

According to the World Economic Forum's Global Risk Landscape 2018, part of its Global Risk Report (GRR) 2018, both cyber-attacks and data theft are two of the topmost risks to the world we are living in, ranking next only to extreme weather events and natural disasters in terms of likelihood. Cyber-attacks are also the 4th most impactful risk.

That pretty well explains why organizations are worried and want to do something. That also explains why the regulators are worried and want to do something—which, in turn, means asking the organizations to do those 'extra' things. Rapid digitization of more and more functions, evaporation of the boundary between digital and physical (and increasingly biological) means that these 'somethings' have to be done pretty fast.

All these, in a typical commercial organization of some size, converge at the desk of the head of information security—often called Chief Information Security Officer (CISO) these days.

The function itself is not new; the brief is fairly new.

And it is fairly simply – it reads protect and comply. Yes, while the final objective is 'protect', 'comply' is a very significant independent objective. To protect, you must do what is right. To comply, you must also do what the regulator thinks is right. Never mind, the objectives are the same.

All that this not-so-comprehensive survey asked CISOs are some simple questions—their reporting, what they spend time on, their involvement in purchase, their challenges—and to complete, the deployment status of various security solutions and their expectation from the security vendors.

> **The survey asked the CISOs the scope of their responsibility... That could actually give a clue to how many, GDPR actually matters.**

This survey was conducted among CISOs attending our annual CISO Forum on a day that was an important date in the recent lives of CISOs worldwide—May 25, the day GDPR kicked off.

It is not trivia info. The survey asked the CISOs the scope of their responsibility—whether it is restricted to India, to regional levels or global levels. That could actually give a clue to how many, GDPR actually matters.

The objective of the survey was to simply get a little more insight into the changing scope of a CISO's work.

While there is a significant change over the years, to those tuned in, many findings should not come a surprise. For example, the fact that top challenges identified by the CISOs are integration of multiple solutions and conforming to so many new regulations. Now, who, in security community would find it a 'significant' new finding? Well, next time you converse about it, you can use the data to support your point. That is about it.

Yet, there are some surprises. If you are not surprised, tell us. We know the CISOs' profiles within organizations are rising. But even then, it came as a surprise that those reporting to people outside IT organizations outnumber those part of IT organizations by eighteen percentage points! ■

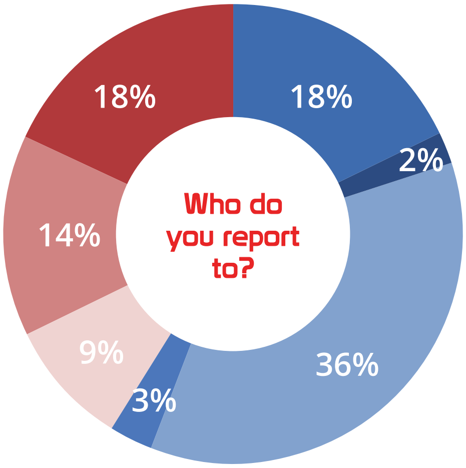
Let's start with that.

READ ON...

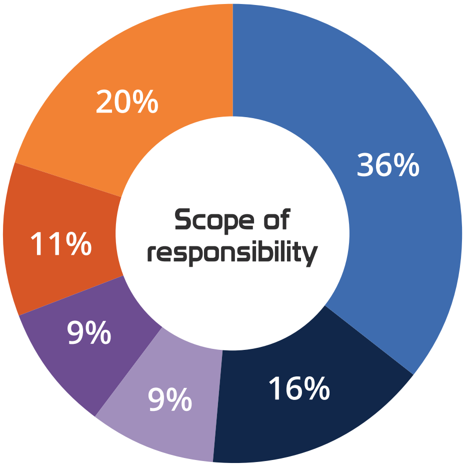
Changing reporting structure reflects changing priorities

That more security leaders now report to Corporate Risk or top management is, as compared to just three years back, no surprise. But what the survey tells us is that more security leaders now report to Corporate Risk or top management as compared to those who report to IT. And that difference is significant. This should leave no doubt in anyone's mind about the importance Indian organizations have started giving to information security.

🟦 CEO/Managing Director/ President
🟦 CFO/Finance Director/ Finance Controller
🟦 Chief Risk Officer
🟦 COO
🟥 VP/GM-IT
🟥 CTO/Head oof IT Infra/ Head of IT Operations
🟥 CIO/Group CIO



Source: CSO Forum 2018 CISO Survey



Source: CSO Forum 2018 CISO Survey

Well, not every regulation is for everyone

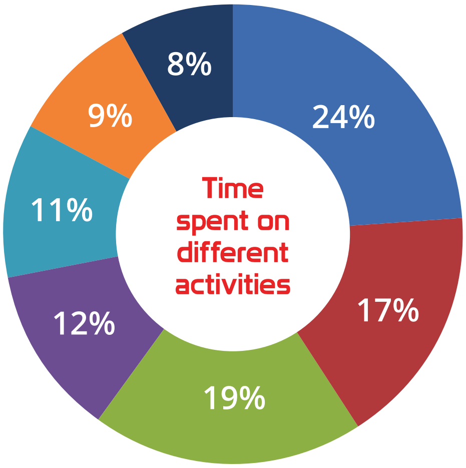
Considering that compliance is now a major responsibility of the CISOs; geographic scope is becoming more and more important. For example, this data shows that a maximum of 31% could potentially be responsible for acting on GDPR, as only their scope is global. We say maximum because there may be many focused on North America alone, for example!

🟦 Single Company,India only
⬛ Multiple Companies, India Only
🟪 Single Comapany, Regional International
🟪 Multiple Companies, Regional Internatioinal
🟧 Single Company, Global Scope
🟧 Multiple Companies, Global Scope

It's a lot more strategy now!

Almost one-fourth of the time is spent on making security strategies. With operational security now mostly part of IT teams and the information security leader in the Corporate Risk team, this is but a logical expectation.

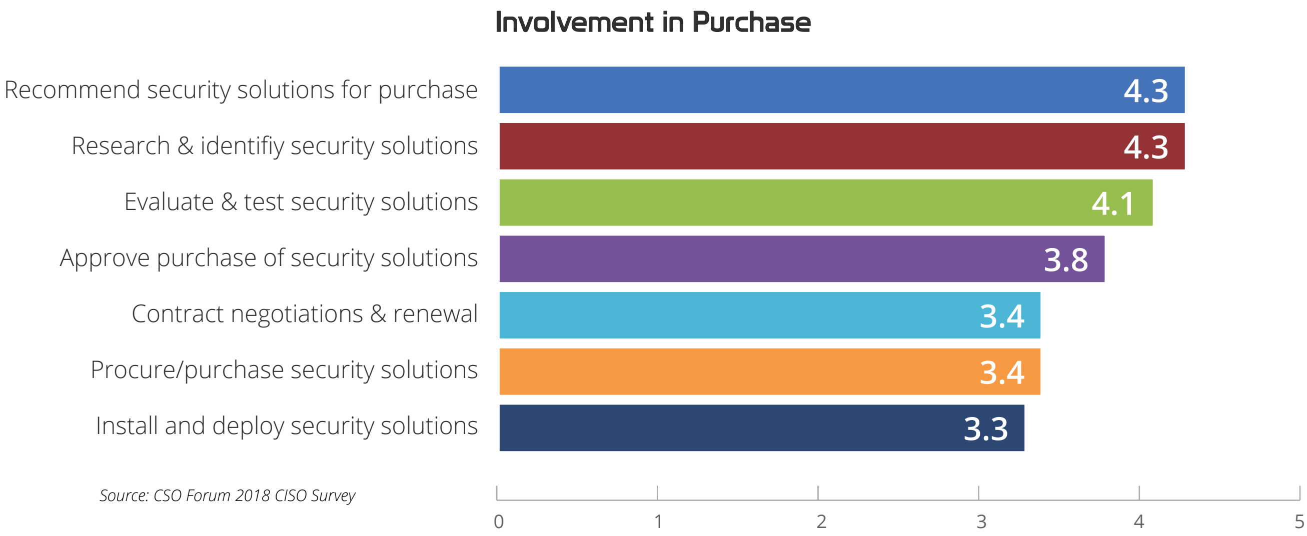
🟦 Security Strategy
🟥 Technology Evaluation & Selection
🟩 Security Operation Management
🟪 Security Training & Education
🟦 Vendor and Supplie Management
🟧 Contracting & Negotiation
⬛ Other



Source: CSO Forum 2018 CISO Survey

It’s much less of implementation work

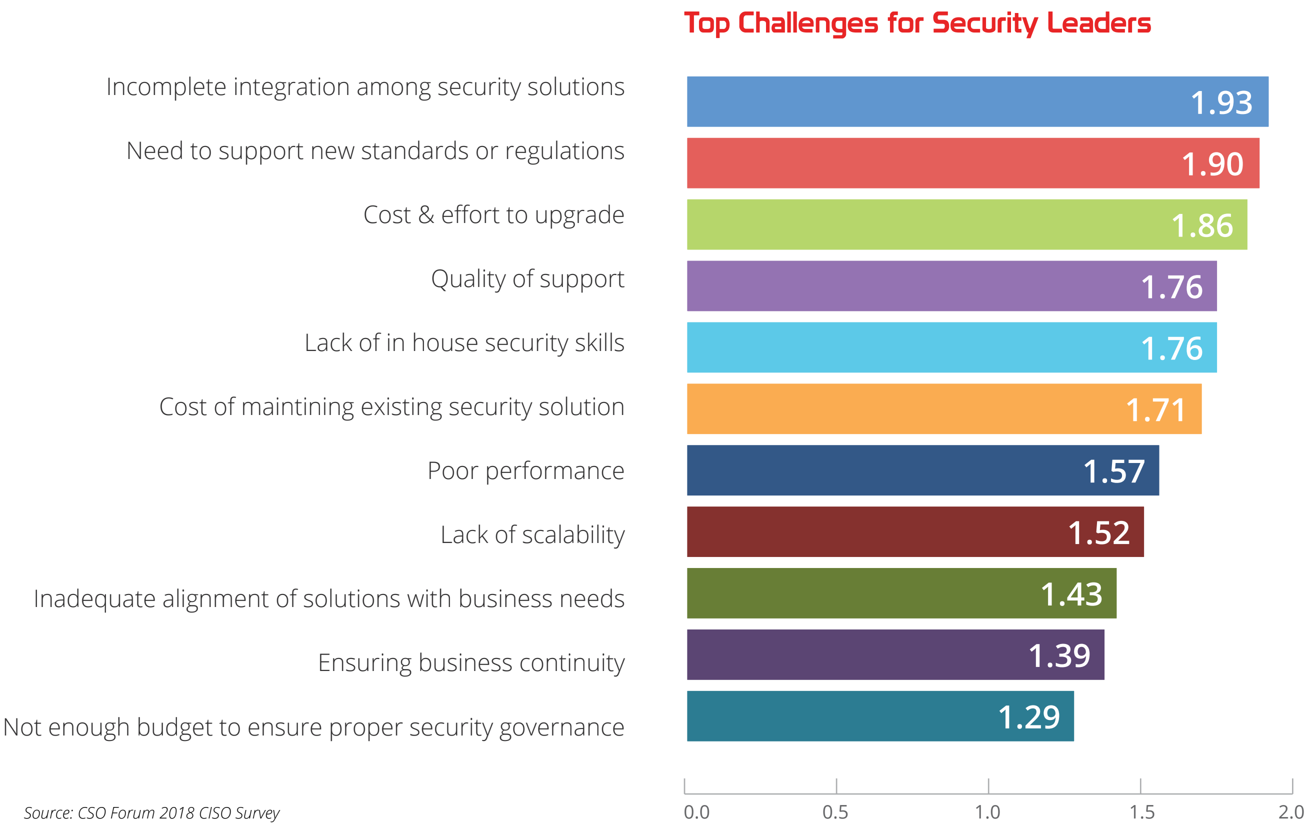
Despite security leaders moving into the Corporate Risk, most security solutions are still decided and/or heavily influenced by them. They still evluate, even test solutions. Implementation is a different thing, though.



Source: CSO Forum 2018 CISO Survey

Oh, I C (Integration-Compliance) the challenge

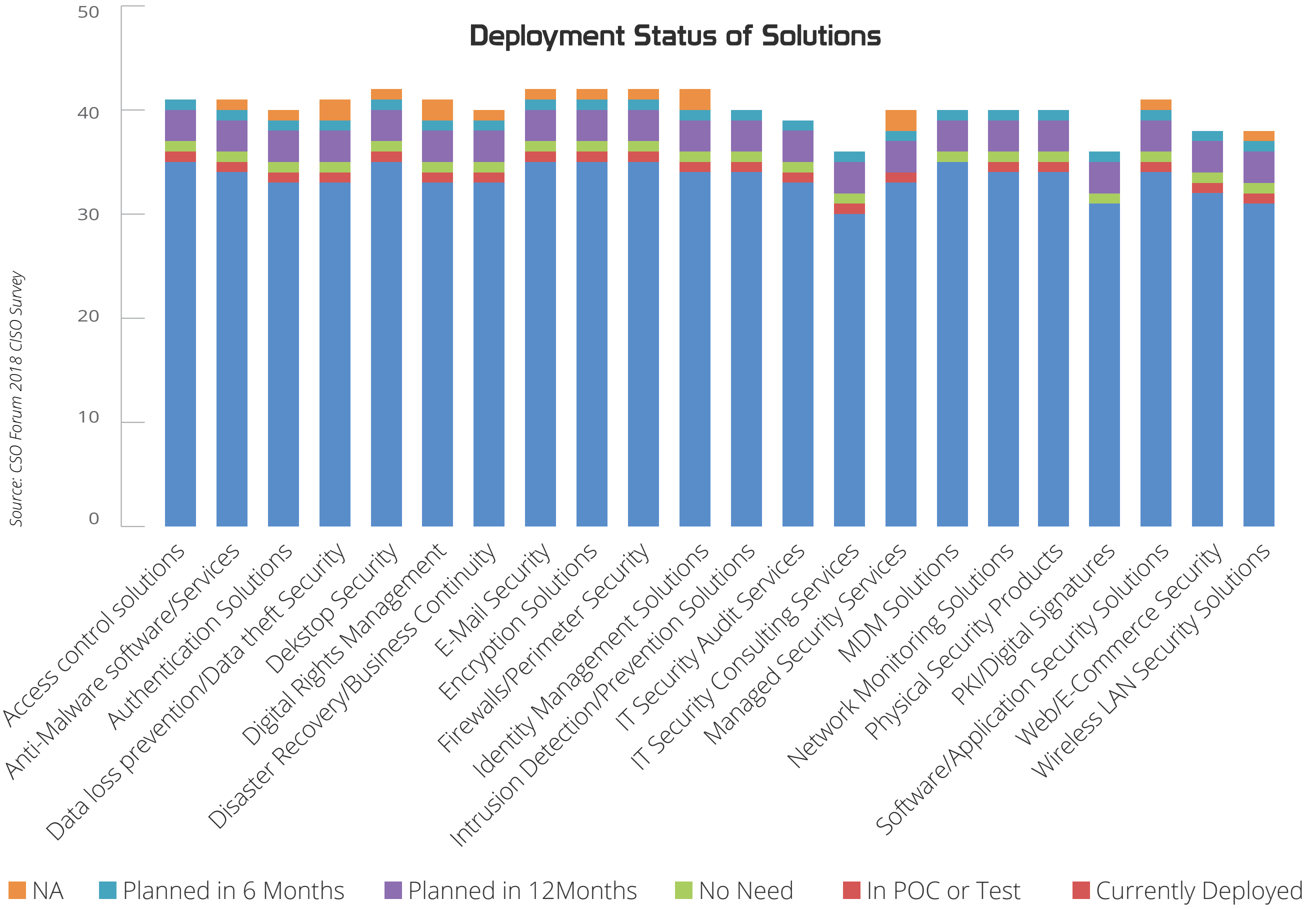
Probably the clearest indicator of what security leaders are up to, this one should come as no surprise. While integration of multiple point solution to make the defence more effective is something that remains the top challenge, compliance is right there at No 2. Will you be surprised if it moves to No 1?



Source: CSO Forum 2018 CISO Survey

Well, tech solutions are in place, by and large

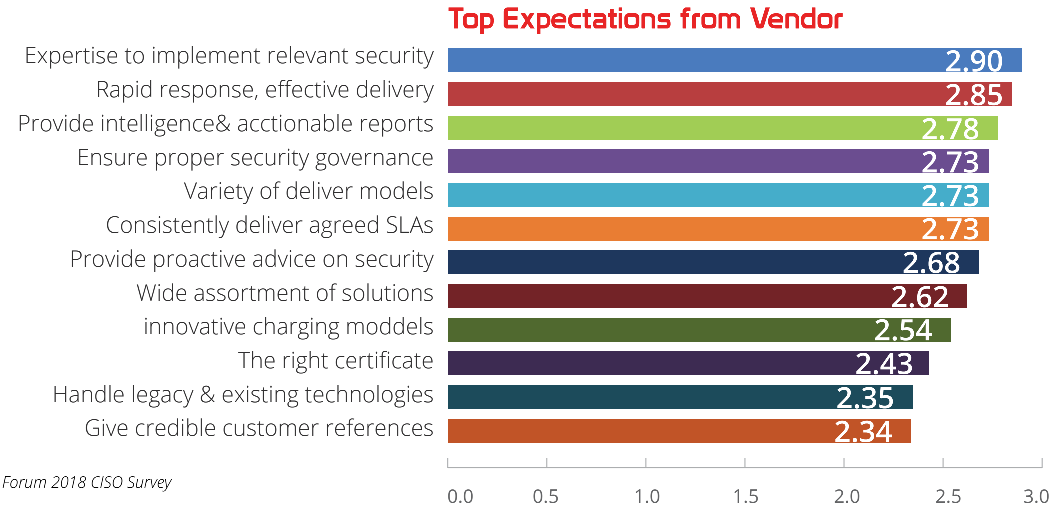
Almost all tech solutions have more than 80% penetration. Yet, if the security market is such a vibrant place, give the bad guys some credit. Also, a pertinent question to ask – is the whole delivering a value that is greater than, equal to, or even less than the sum of parts? The preceding chart – the challenges – can give you a clue!



Source: CSO Forum 2018 CISO Survey

Good delivery – not tall promises–expected from vendors

Actually, expectation from vendors is simple. Deliver what you say. Implement, respond...and give some intelligence. The third point is becoming stronger year after year. What was once a differentiation is now hygiene.



Source: CSO Forum 2018 CISO Survey

19th CIO&LEADER CONFERENCE

THE PRACTICAL CIO

AUGUST 10-12, 2018 | HOLIDAY INN, GOA

Enjoy a sumptuous **Goan Cuisine** on the banks of River Sal

Tap your feet to the **Retro beat**

Win Big at **The Casino**

PILLAR PARTNER Microsoft | PLATINUM PARTNER FUJITSU | GOLD PARTNERS Adobe paloalto NETWORKS | SILVER PARTNER f5 | ORGANISED BY CIO&LEADER | A BRAND OF 9.9 GROUP

RSVP: **Abhishek Jain**
abhishek.jain@9dot9.in; +91 9312119363

#CIOAnnual #PracticalCIO

EXTRA Curricular

Sachin Shenvi believes in Communion with nature.

Trail Mix

NEXT100 Winner 2016 **Sachin Shenvi**, Manager - IT, Mahindra & Mahindra, shares his intense passion for trekking. Besides, he also takes a keen interest in social activities, for example helping out underprivileged children.

"I took the one less travelled by, and that has made all the difference"
– Robert Frost

"Do not follow where the path may lead. Go instead where there is no path and leave a trail."
– Ralph Waldo Emerson

"In every walk with nature, one receives far more than he seeks"
– John Muir

"Because in the end, you don't remember the time you spent working in the office or mowing your lawn. Climb that goddam mountain."
– Jack Kerouac

I belong to Maharashtra, the land of King Shivaji, who is my idol. He did so much for the state, from building forts in plainlands to high altitudes. His trekking trails, especially in remote and dangerous locations encouraged me to take up this amazing activity.

I actually started trekking in college and joined a group called 'Student Welfare Academy'. They not only help economically not-so-strong students, but also involve them in various physical activities and adventure sports. When I started getting more

Sachin Shenvi

Snapshot

NEXT100 Winner 2016 **Sachin Shenvi** is currently working as Manager – IT in Mahindra & Mahindra. He has done his PG Diploma and Diploma in Management Studies as well as Diploma in Engineering and Technology. He has also done his certification in Harvard Manage Mentor from Harvard University.

and more involved with them, I gradually developed that passion within me. Although I was doing well and my family background was financially sound, I still got involved in their social activities and trekking was an integral part of it.

I usually did most of my trekking in the monsoon season and my first trek with the academy was in Bhimashankar in 1998. The altitude of the place is 5,000 ft. I walked all the way up and enjoyed the greenery and the serene atmosphere.

However, my most challenging trek was Kalsubai, the highest and the steepest peak in Maharashtra. I successfully trekked up and this was a real achievement for me.

Trekking helps me come closer to real nature. It takes me to an entirely different world. It helps me completely forget the outside world, the daily stress and also helps me communion with the beauty of nature. Moreover, it actually helps one's body and is a perfect exercise. For instance, patients with asthma can benefit from trekking in the long run, as it can make their lungs strong.

Last but not least, my advice to people interested in trekking is that if one can manage to climb up a mountain and just look around, the feeling he/she will sense is simply amazing!

One should just feel, experience and enjoy nature closely, rather than sitting at home and doing nothing. Once a person starts such kind of activity, he/she is bound to receive a different kind of pleasure. Also, more than money, one should take care of one's health and trekking is the perfect tonic to stay fit and active! Being fit will automatically help in one's professional and personal life and so everything is linked.

So, just go for it! Trek on! ■

Inspired by Shivaji, Sachin follows his trail.

As told to Dipanjan Mitra, Team ITNEXT

```
h3 {font-size: 20px !important;}
th {font-size: 11px; text-align: left;}
hr {margin: 3px !important; padding: 0px !important; padding-top: 5px !important; border-top: 1px solid #ccc !important;}

#container {margin: auto; width: 850px; padding-top: 90px;}

#info_bar_line1 {font-weight: bold; font-size: 20px; margin: 0; padding: 0; text-align: left;}
#info_bar_line2 {font-size: 14px; margin: 0; text-align: left;}
.info_bar {width: 100%; background-color: #428BCA; position: fixed; padding: 10px 20px; z-index: 10;}
.info_bar p {color: #ffffff !important;}

.hide {display: none;}

.field_information {cursor: pointer; float: left; margin: 1px 0 0 5px;}
.field_information_container {float: left; }
.label {font-size: 82% !important;}
.btn_copy_text {width: 110px;}
#btn_get_first {width: 110px;}

.title {width: 701px !important;}
.description {width:701px !important; height: 73px !important;}

.tag-editor {line-height: 25px !important; height: 225px; padding: 5px 0px !important; border: 1px solid #ccc !important; border-radius: 4px; overflow: auto !important;
.tag-editor-delete {height: 25px !important;}
.tag-editor-delete i {line-height: 25px !important;}
.tag-editor-spacer {width: 10px !important;}

#btn_settings {-webkit-user-select: none; -khtml-user-select: none; -moz-user-select: none; -ms-user-select: none; user-select: none; transition: all 0.5s ease-out 0s;}
#btn_settings:hover {cursor: pointer;transform: rotate(360deg);transition: all 0.5s ease-out 0s;}

#select_theme_container {width: 280px;}
#google_api_key {width: 400px;}
#get_first_n_value {width: 50px;}
.simple_text {text-decoration: none !important;}
.panel-settings {padding: 10px !important;}
.panel-settings-container {margin-bottom: 5px !important;}

#google_translate_api_info {font-size: 10px; margin-left: 25px;}
.checkbox_comment {font-size: 10px;}
.btn-default .badge {margin-left: 3px; border-radius: 8px !important;}
mark {padding: 0 !important;}

#add_and_translate {font-size: 10px;}

.tooltipster-box {background: #fff !important;}
.tooltipster-arrow-background {border-top-color: #fff !important;}
.tooltipster-box {-webkit-box-shadow: 0 1px 4px rgba(0,0,0,.2); box-shadow: 0 1px 4px rgba(0,0,0,.2)}
.tooltipster-arrow{height:10px !important;}
.tooltipster-content {margin: -2px 0px !important; }

#user_language {width: 50px;}
```

Facebook Crisis And Network Security In India

Currently in India, there is no data protection policy or any government policy around it

By Anshuman Singh

A UK based political data analytics firm, Cambridge Analytica allegedly sourced the data of around 80-90 million Facebook users illegally without their knowledge and consent and used it during Donald Trump's presidential campaign. They allegedly started collecting the data in 2014 and used it to form political campaigns and influence voter opinion. Facebook claimed that the users were duped by a researcher who originally got the data through a quiz app hosted on Facebook. However, Facebook's then malfunctioning design allowed this app to not just collect personal information of people who agreed to take the survey, but also the personal information of all the people in those users' Facebook social network. This caused huge uproar not only in the US but also globally. While many deleted their Facebook accounts, everyone else became deeply skeptical about not just Facebook but also online security and data privacy in general.

Cambridge Analytica was doing a lot of number crunching to understand user behavior and preferences, which is very normal, but what caught people's attention is that it was allegedly influencing people's behavior. People are not too careful about what they are posting on social media, what they like on it and if somebody has that data, they can predict your behavioral choices, political leanings, religious leanings and other important factors. The other scary part was that if you are leaning towards their views, they will create more campaigns and content that strengthens your views and if not, they will try to influence your views.

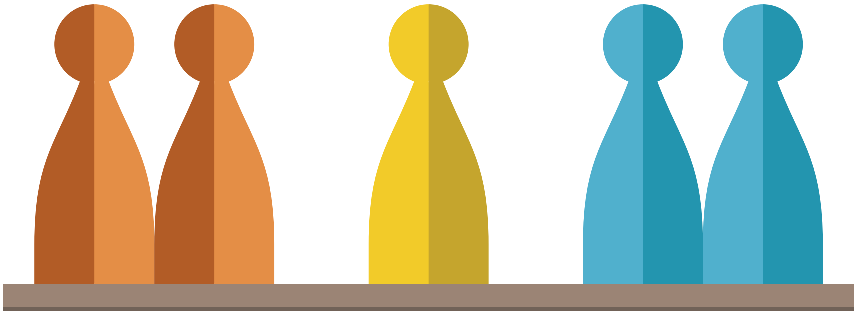
Currently in India, there is no data protection policy or any government policy around it. There should be a way to enforce best practices of data collection, retention and disposal; otherwise it becomes an easy prey not just for hackers but also unscrupulous organizations. Organizations are not bound to secure your data in any way. For example, there are lots of government services for which we can pay online, like water bill, electricity bill, etc. In that case, I am providing my information, and it is the government service provider's duty to keep my data secured and not use my data in any malicious way. While the government service providers may not be selling data but many private companies may be doing that, we need to be careful about the kind of information we put online. They should also be careful about it. In Europe, General Data Protection Regulation (GDPR) policies went into effect from, 25 May 2018, which has put a framework on how data should be secured, retained, utilized and disposed. Deleting old data is an important aspect of the regulation. The European Union (EU) regulation has strict data regulation rules. Each individual has the right to go to an organization and ask the organization to delete his/her data. They are bound by law to delete the data within a stipulated time. If you are not compliant, penalties are very high. The presence of a similar law in India will bring a lot of trust back into online transactions.

People are not too careful about what they are posting on social media... and if somebody has that data, they can predict your behavioral choices...

It is also very important for most businesses to keep their customer's data secure. Say, you are an online e-commerce company. You will have customer data, which needs to be kept securely. The other aspect is that after data is stored, you need to ensure that your database is encrypted. There are other threats like encryption malware. Organizations will have all business data and if a ransomware hits and collects the data, it can cause grave consequences. That is where storage backups come into the picture.

The Facebook-Cambridge Analytica crisis has taught the world a huge lesson that at any point we cannot be casual about our online data and we are not yet in a fully secure state. It is rumored and there is no proof that data was used to swing the elections and if that is true it is a big thing. If it was done by a third party, it is even worse. We also need to be aware about certain things when online, like giving permission to apps to access our profile. It seems fun but can cause huge damages. Another thing is distinguishing between real and fake info and we need to be careful in this aspect. ■

The author is Senior Director - Product Management at Barracuda Networks



Majority Of Organizations Ill-Equipped To Manage Third-Party Risk

Over 70% organizations do not have adequate knowledge or required visibility into third-party outsourced relationships

By Sachin Paranjape

No company can function as an island and as our eco system broadens it typically deals with many entities like customers, partners, affiliates and others. When organized together these entities form what we term as the "extended enterprise" which is closer to the core of business than ever before. Organizations that step up to the challenge of developing programs to better manage this risk can elevate their position in the market by unleashing with confidence the reach, expertise and relationships that third parties can bring.

Third party risk management has to become a top-of-mind priority for organizations. In this respect, our recent (third) annual EERM (Extended Enterprise Risk Management) survey, based on 975 responses from a variety of organizations across 15 countries of Asia Pacific, Americas, Europe, Middle East and Africa region, has highlighted some interesting findings. 70% of organizations in India recognize an increase in risk but remain ill-equipped to deal with it because of inadequate or absolutely no knowledge of sub-contractors engaged by their third parties. In fact, 14% of the respondents in the survey stated that third party-outsourced relationships are not identified, monitored or reviewed at all.

Companies today have to rely on relationships that are multiple and third party in nature, and typically outsourced. These are like outliers on the risk periphery – even for organizations that place strong focus on risk. Our survey report highlights the below key areas where organizations could benefit from further effort:

- **Controlling heightened risk:** Dependence on third parties continues to grow, with over 70% of Indian respondents stating that their dependence on extended enterprise has grown owing to business and macroeconomic conditions. Impact of external events (42%) and increasing threat of their party related incidents and disruptions were the two most dominant factors contributing to the perception of heightened risk in the extended enterprise.
- **Enhanced board engagement:** Board oversight and engagement with EERM programs continues to lag. At a global level, 78% of organizations suggest that the Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Procurement Officer (CPO), CRO, or a member of the Board is ultimately accountable for this. In India, this decision rests with the Chief Procurement or the Risk Officer. Boards in India are making relatively slow progress on this matter whereby 57% of the respondents suggested that their boards merely have a moderate level of understanding and engagement on this subject.
- **Technology platforms:** In keeping with the trend of increased centralized oversight of EERM activities, technology decisions are now being taken more centrally and standard tiered technology architecture is emerging. Less than 10% of our global respondents in our survey are currently using bespoke systems for EERM, a sharp drop from just over 20% last year.
- **Sub-contractor risk:** Organizations lack appropriate visibility of sub-contractors engaged by their third-parties as well as the discipline and rigor to frequently monitor such fourth/fifth parties. 57% of survey respondents feel they do not have adequate knowledge and appropriate visibility of sub-contractors engaged by their third-parties and a further 21% are unsure of their oversight practices. ■

The author is Sachin Paranjape, Partner, Deloitte India

Majority Of ITDMs Say Compliance Worries Restrict Their Cloud Usage: Survey

63% felt the need to use multiple infrastructure management tools was also a hugely restricting factor in their use of multiple cloud vendors

87% ITDMs limit their use of the cloud because of the complexity of managing regulatory compliance, according to a study by WinMagic. A quarter (24%) said, it meant as a result, they only work with a single cloud vendor in their infrastructure, rather than exploit the benefits of a multi-cloud environment, such as cost effectiveness, flexibility, reliability, security and avoiding vendor lock-in.

Hands tied by management tools

The survey, which included ITDMs in Germany, India, the UK and US, also noted that 63% felt the need to use multiple infrastructure management tools was also a hugely restricting factor in their use of multiple cloud vendors.

Looking specifically at managing security compliance across the enterprise, over a quarter (28%) stated they would "not be completely confident" IT systems met all the required processes and standards if an audit was called "today". 7% went as far as to say there was "a high risk of them failing."

Good security compliance benefits highlighted

On the positive-side, platform-agnostic management tools that enable enterprises to implement solid security and compliance policies across on-premises and cloud providers are bringing proven benefits. ITDMs reported a number of benefits in terms of efficiency and cost savings:

- 63% improved the efficiency of their systems
- 57% now had enforced compliance across the infrastructure
- 56% say they are more secure
- 32% have made measurable cost savings
- 30% believe their risk exposure is lower

"The benefits of good security management tools are clear in the survey, but the pain caused by poor tools even more so, with companies restricted on their infrastructure choices and placed at greater risk of regulatory fines," said Mark Hickman, Chief Operating Officer at WinMagic. "But poor security compliance is so much more dangerous, putting company data at risk of data breaches, both accidental and through theft, by hackers or even employees. WinMagic SecureDoc CloudVM offers a common platform with less complexity, more flexibility and that is highly secure on the widest range of virtualized and cloud environments, freeing ITDMs to pursue a multi-cloud mixed infrastructure and all the benefits that come with it."■

India Inc Envisages GDPR As The Next Big Business Opportunity

71% Indian enterprises say GDPR will help bring a sense of privacy in business and innovation in ideas

71% Indian enterprises say Global Data Privacy Regulation (GDPR) will help bring a sense of privacy in business and innovation in ideas, according to a recent survey conducted by Deloitte Touche Tohmatsu India LLP (DTTILLP or Deloitte India or Deloitte) in alliance with Data Security Council of India (DSCI).

The joint study reaffirms, organizations that are GDPR ready will gain a competitive advantage, as they will be able to use personal data in their innovations and digitization, helping provide better delivery to their clients through the following measures:

- Provide better customer experiences (60%)
- Enhance productivity of internal operations (54%)
- Personalization of product & services deliveries (47%)
- Creation of new products and services (46%)

In addition, particularly small & mid-size EU companies would open up for business possibilities to Indian firms, given the ease of data transfer between organizations.

With respect to sectors, IT/BPM, Health, Ecommerce, Manufacturing and Pharma are the five frontrunners of the GDPR readiness journey.

Commenting on the survey launch Vishal Jain, Partner, Deloitte India said, “Digital transformation and advanced technologies have enabled enterprises to enhance customer experience. This requires a fair balance between data privacy and accessibility.

GDPR brings in a renewed focus on data privacy. While this is a new compliance imperative, it also provides a competitive advantage to businesses. In fact, our survey findings also infer that GDPR can be the new business opportunity for Indian firms.

The need of the hour for India Inc is to develop a strategic roadmap of adoption for this policy that is transparent and further allows them to build the next layer of customer trust.”

Rama Vedashree, CEO, DSCI said “EU has been a key geography for Indian IT and has been servicing customers across several verticals including public sector.”

Innovations in global services delivery models, best in class processes and standardization, attention to data protection has kept India’s IT growth story flying high. Scaling its people, process maturity and harnessing technology solutions for rigorous implementation has enabled driving conformance to data protection regulations in various geographies. Given EU GDPR, and impending India’s Data Protection Law, stepping up focus on Data protection practices and capability building, is a key imperative to satisfy expectations of customers and consumers.

The joint survey from Deloitte and DSCI is an effort to analyse the current state of preparedness of Indian organizations basis the requirements mandated by the European Union’s (EU) General Data Protection Regulation (GDPR).

■ According to the survey in India, even as 28% of the small organizations are yet to initiate their journey towards GDPR, 71% of survey respondents expressed that this regulation will help bring a sense of privacy in business and innovation in ideas.

■ Out of the organizations that have taken action for GDPR readiness, 80% have conducted general awareness campaigns for all their relevant stakeholders to identify their processes, which access personal or sensitive data.

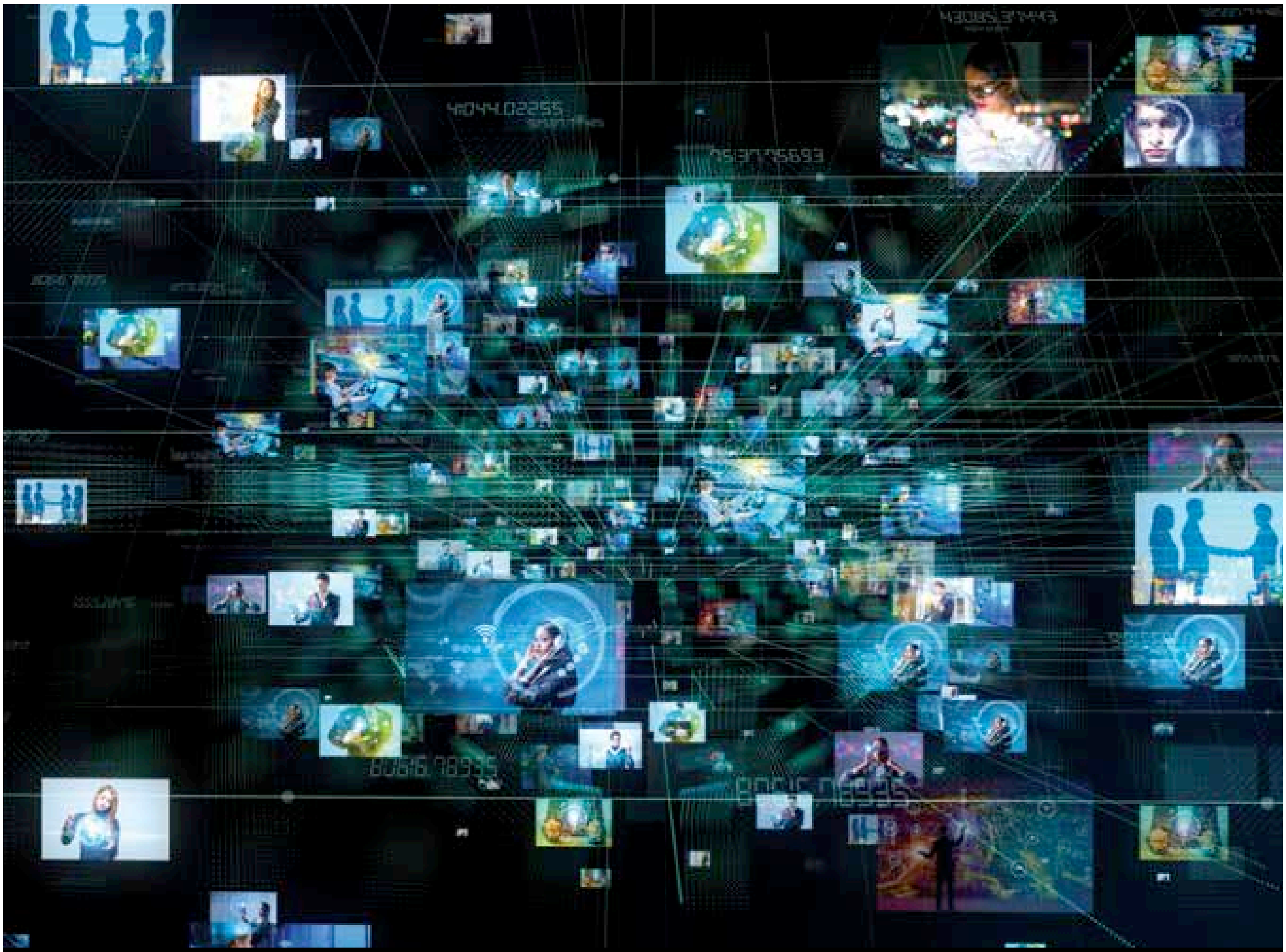
■ While Right to Data Portability, Right to Erasure and Right to Restriction of Processing were recognised as most challenging data subject rights, 62% of respondents felt avoiding legal & contractual liabilities, fines & penalties as the biggest motivator for compliance followed by the need to get a competitive edge.

■ The report also notes that IT/BPM sector was the most responsive sector in terms of taking any steps towards GDPR readiness with 84% of IT organizations having started readiness journey. This was followed by health and E-commerce sectors with 81% and 80% organizations respectively initiating their process.

As a step forward, this survey laid emphasis on the need for a dedicated privacy team and a Data Protection officer (DPO) as their absence may pose a problem for organizations once the regulations for data privacy of various countries broaden after the enforcement of GDPR. This team would set the ground for Data Protection Impact Assessment (DPIA) that would help organizations identify, assess, and mitigate or minimize privacy risks with data processing activities.

Furthermore, it suggest that it is important for Indian organizations, especially Business Process Management (BPM) organizations, call centres and Business Process Outsourcing (BPO) organizations, to assess their role under GDPR as that of a Data Controller (DC), Data processor (DP) or both, since regulatory requirements for a Data Controller may vary from those for a Data Processor..■

GDPR brings in a renewed focus on data privacy. While this is a new complinace imperative, it also provides a competitive advantage to businesses. In fact, our survey findings also infer that GDPR can be the new business opportunity for Indian firms



State of Martech 2018

Data analytics and artificial intelligence have brought about sweeping changes in the marketing technology landscape. We share here insights from Walker Sands Communications' State of Marketing Technology 2018 report

If one business function is changing dramatically because of the rapid strides in data analytics and artificial intelligence, then it is marketing. Technology has changed not just the effectiveness, but also the scope and accountability in marketing.

So, how are marketers using technology? Walker Sands Communications' ***State of Marketing***

Technology 2018 report, prepared in association with Chiefmartech.com provides insights into the state of affairs in marketing technology (martech).

The big message: with a lot of niche players, marketing technologies (martech) are seeing a significant pace of innovation. Despite updating their martech stack at least once every six months, marketers still struggle to keep pace with the rate of technology change.

"Most marketing organizations still cannot implement solutions at the same rate that the technology evolves, or in pace with their own hopes for the future," says the report.

However, marketers are sensitized about this and hence assess their martech stacks at far regular intervals than they used to do a year back.

Here are some topline findings:

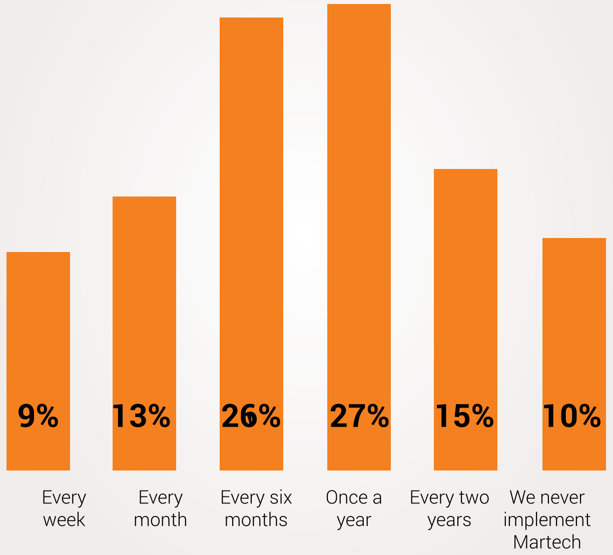
- Marketers have rejected the "set it and forget it" philosophy. 52% of marketers assess their martech stacks at least every six months.
- Marketing organizations will increase their martech budgets. 65% of marketing organizations say they plan to increase their spend on martech in the next year.
- Marketing organizations can't keep up with the rate of martech innovation. 63% of marketers feel the martech landscape has evolved rapidly or at light speed in the last year, while only 28% feel the same about their company's use of martech.
- The future of marketing requires both technology and creativity. 56% of marketers believe an equal mix of creativity and technology will drive marketing strategies five years from now.

Now, into some more detailed look at the findings:

- Every three out of four marketers say they add to their organization's marketing technology stack in one year or less. It is almost continuous upgradation.
- When the pace of change is so fast, there is a need to holistically take a stock as frequently as possible. Again, 76% say they do it at least once a year.
- Yet, most feel they are failing to match the pace of evolution in martech
- Needless to say, most are upping their martech budgets
- But most are confident of their skill levels
- IoT is first among equals when it comes to adoption among emerging technologies
- Video marketing seems to be the hot new application that will get deployed this year but there are many more... ■

Chart 1: How often does your company add new tools to its marketing technology stack?

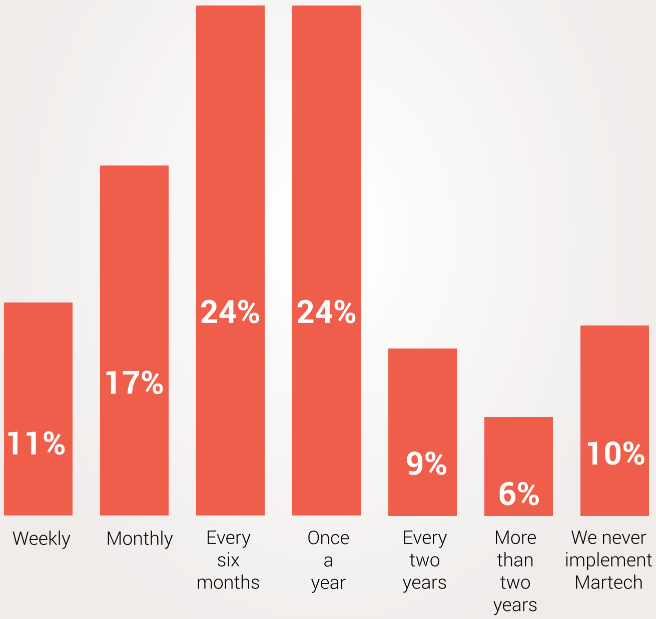
Periodicity of Martech Updates



Data source: State of Marketing Technology 2018 by Walker Sands

Chart 2: How often does your company assess its marketing technology stack holistically?

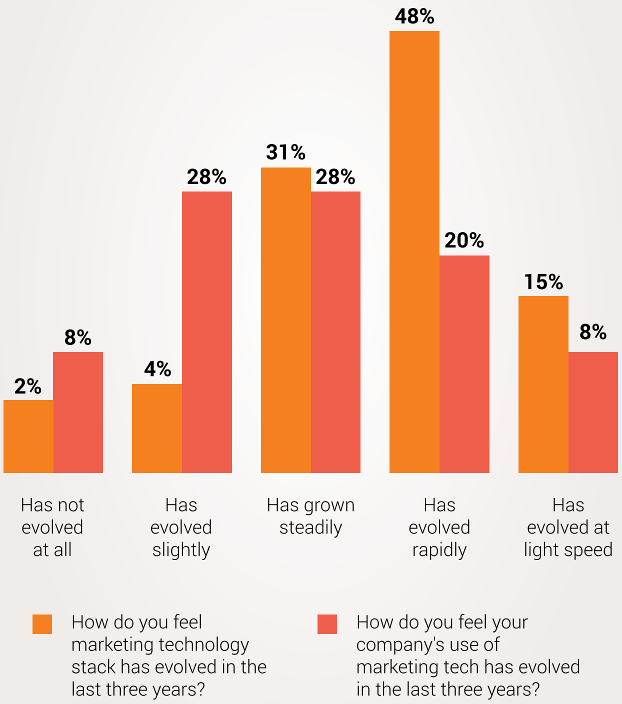
Periodicity of Holistic Assessing



Data source: State of Marketing Technology 2018 by Walker Sands

Chart 3: How do you feel marketing technology stack has evolved in the last three years? How do you feel your company's use of marketing tech has evolved in the last three years?

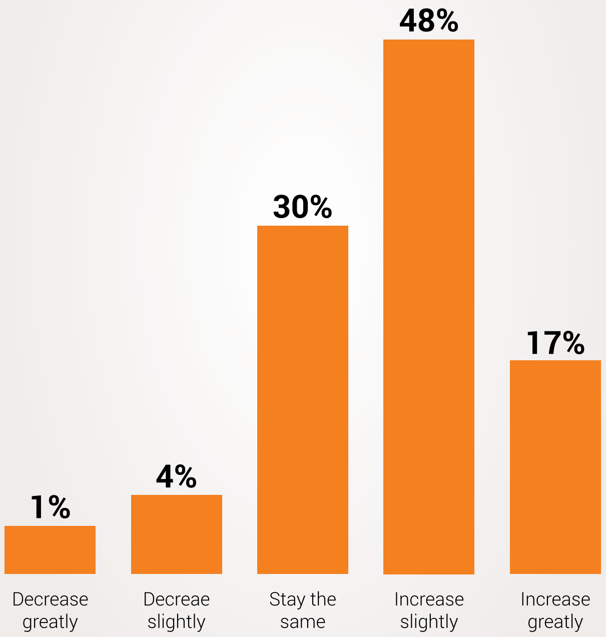
Evolution and Usage of Maretch



Data source: State of Marketing Technology 2018 by Walker Sands

Chart 4: How do you expect you company's martech budget and investment to change in 2018 as compared to 2017?

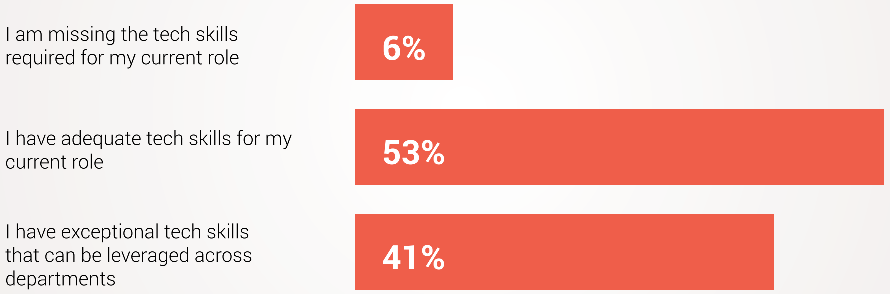
Company's Martech Budget in 2018 as Compared to 2017



Data source: State of Marketing Technology 2018 by Walker Sands

Chart 5: Which of these statements best describes how your skills line up with the technology needs in your marketing department?

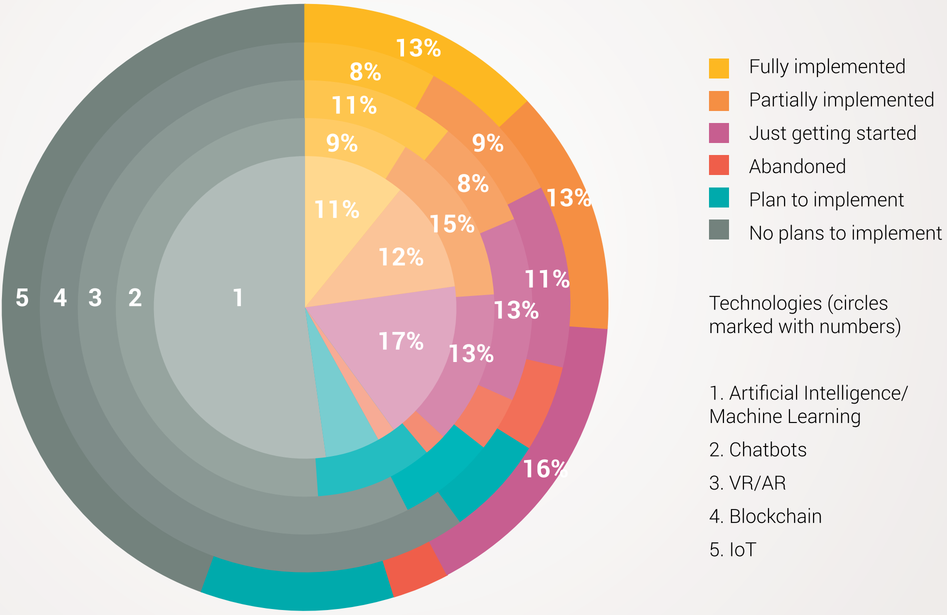
Personal Skill Assessment



Data source: State of Marketing Technology 2018 by Walker Sands

Chart 6: At what stage of implementation is your company with the following technology as part of your marketing strategy?

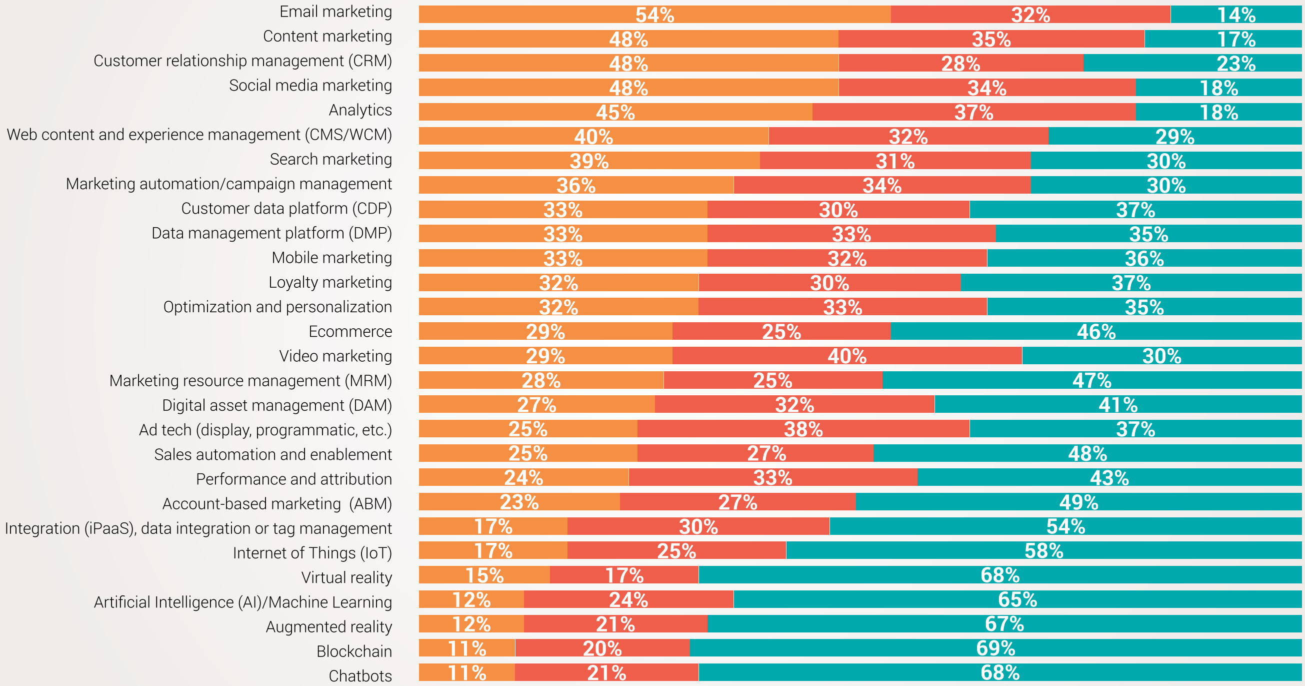
State of Emerging Technologies Adoption by Marketers



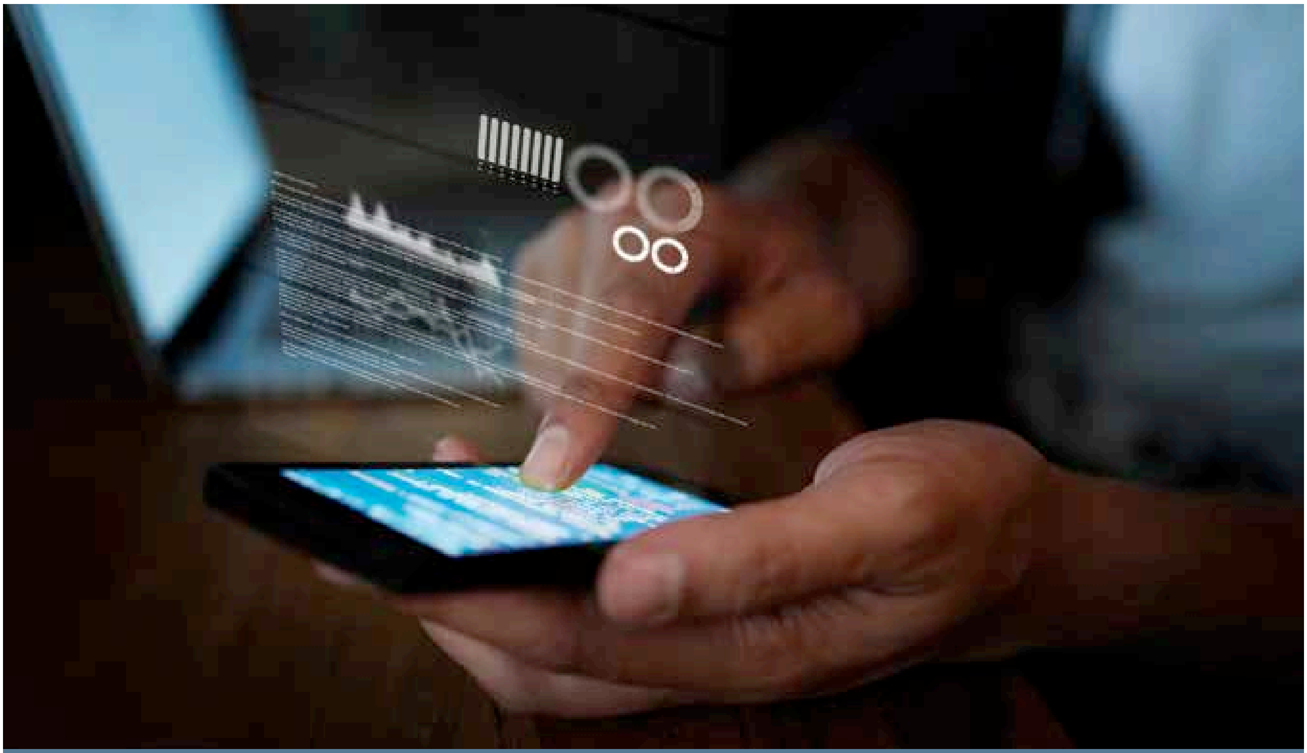
Data: Walker Sands State of Martech 2018

Chart 7

Martech: What's In, What's Getting In?



Data: Walker Sands State of Martech 2018



Majority Of Digital Workers Say Their CIOs Are Unaware Of Their Technology Needs: Gartner

According to Gartner, less than 50% of workers (both IT and non-IT) believe their CIOs are aware of digital technology problems that affect them

As many IT workers develop greater technology skills and apply them to advance their careers, many digital workers in non-IT departments believe their CIO is out of touch with their technology needs. According to Gartner, less than 50% of workers (both IT and non-IT) believe their CIOs are aware of digital technology problems that affect them.

The survey further revealed that European workers said that their CIO is more aware of technical challenges (58%) than U.S. workers believe they are (41%).

“Non-IT workers aren’t likely to use the IT help desk as their first source of assistance, and are less likely to believe in the value of their IT organization," said Whit Andrews, vice president and distinguished analyst at Gartner. "Only one in five non-IT workers would ask their IT department to supply best practices for employing technology."

The survey also revealed that millennials were less likely to approach IT support teams through conventional means. About 53% of surveyed millennials outside the IT department said that one of their first three ways to solve a problem with digital technology would be to look for an answer on the internet.

Non-IT workers were overall more likely than IT workers to express dissatisfaction with the technologies supplied for their work. IT workers express greater satisfaction with their work devices than do workers outside IT departments. Only 41% of non-IT workers felt very or completely satisfied with their work devices, compared to 59% of surveyed IT workers.

"Many IT departments will be more successful if they are able to provide what workers say they need, and provide inspiration so they can increase the workforce's digital dexterity," Andrews added.

> **The survey revealed that millennials were less likely to approach IT support teams through conventional means...one of the first three ways to solve a problem with digital technology would be to look for an answer on the internet.**

IT Workers Feel More Confident

IT workers feel more confident than non-IT workers at using digital technology. The survey found that 32% of IT workers characterized themselves as experts in the digital technologies they use in the workplace. Just 7% of non-IT workers felt the same. "While we expect IT people to feel more confident with digital technologies, these findings highlight how hard it is to help non-IT workers feel as digitally dexterous as IT workers do," said Andrews.

67% of non-IT workers feel that their organization does not take advantage of their digital skills. "Organizations seeking to mature and expand their digital workplaces will find that expanding digital dexterity will accelerate this across the organization," added Andrews.

Digital Technology Satisfies 72% of Digital Workers

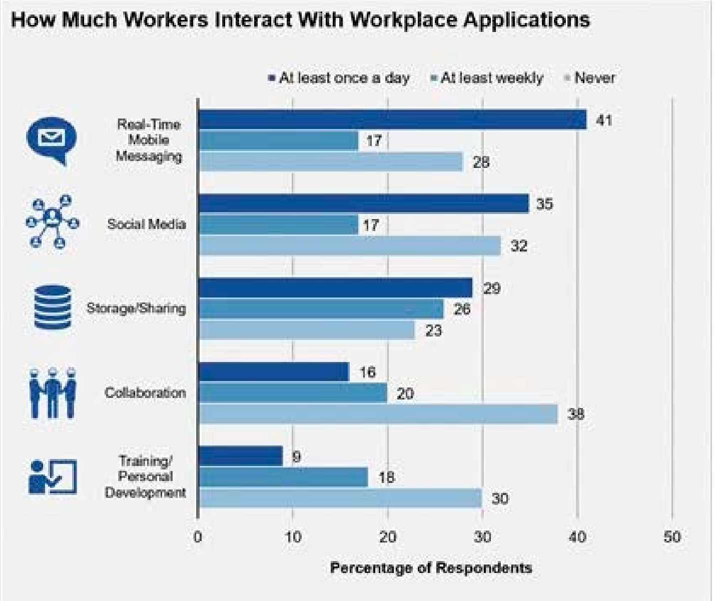
About three in four digital workers either somewhat agree (48%) or strongly agree (24%) that the digital technology their organization provides enables them to accomplish their work.

The most common types of workplace application used by survey respondents were real-time messaging (58%), sharing tools (55%), and workplace social media (52%) (see Figure 1).

However, significant distinctions exist in the workplace. "Millennial digital workers are more inclined than older age groups are to use workplace applications and devices that are not provided by their organization, whether they are tolerated or not," said Andrews. "They also have stronger opinions about the collaboration tools they select for themselves. They are more likely to indicate they should be allowed to use whatever social media they prefer for work purposes."

In addition, relative to the total workforce, a larger proportion of millennials consider the applications they use in their personal lives to be more useful than those they are given at work. "Our survey found that 26% of workers between the ages of 18 and 24 use unapproved applications to collaborate with other workers, compared with just 10% of those aged between 55 and 74," Andrews said.■

Figure 1. The Shape of Workers' Days



Source: *Gartner (June2018)*

Are Indian organizations planning data lakes?

A lot of them are exploring, even as some large banks like SBI and Bank of Baroda go for it. But unlike many analysts, the Indian IT leaders do not take a skeptical view of data lakes

By Shyamanuja Das

When you search for data lake on Google, the first suggestion that is thrown up is—are data lakes fake news? That could give you an idea the extent to which the opinion is divided on data lake's utility—or the lack of it.

Data lake is probably the only trending technology proposition that has so many staunch critics, many questioning the concept itself, even as most vendors advocate it. While some question the mindless roll out—while agreeing that it has got some value proposition for some companies, if done right, others reject it outright.

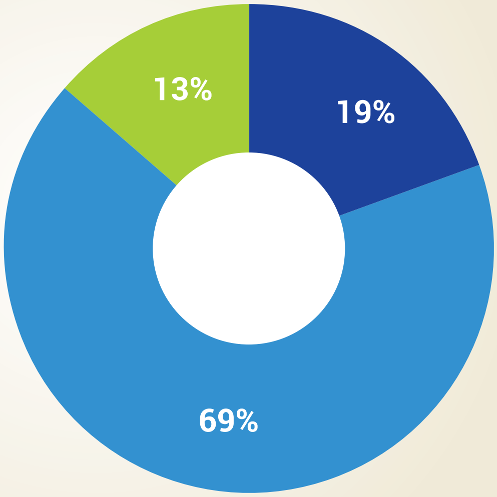
Data lakes are supposed to be large stores of data that could and must store everything, unlike data warehouses where a large amount of data may be rejected. The structuring of the data is pre-defined. So, data lakes are usually designed to support all data types and all users—the end-users who want immediate analysis, the analysts who want to find out what they could do with it to add value to business and those who want to take decisions based on data, with a broad/vague (depending on which side of the line you stand) idea that the whole is better than the sum of parts.

The guiding principle of data lakes is that no data should go waste just because at any particular time you do not know its utility or do not have the capability to draw any meaningful insight from it. Sounds like an advice given by a senior to an intern not so enthused by the mundane task at hand? Well, it is just the beginning (no pun intended).

What kind of organizations should go for data lakes? Of course, those that have a lot of data and have the capability to execute it successfully. If the second condition sounds recursive, it just points to this—wet your feet or just keep aside.

Current set-up: More than two-third IT leaders said they have a centralized data warehouse. A significant number—one in five—said they have no data warehouse.

What out of the following statements best describes your organization set-up?

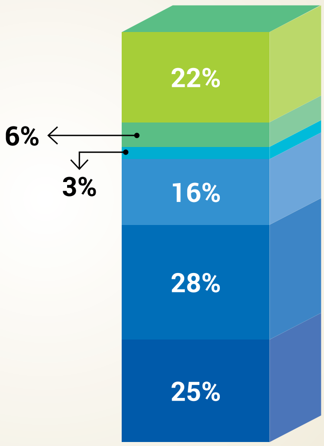


- 🟦 We do not have a data warehouse
- 🟦 We have a centralized data warehouse
- 🟩 We have data warehouses in each of the SBUs

Source: 9.9 Group Research

Setting up data lakes: A majority are exploring the option and that is not surprising

Are you going for a data lake?

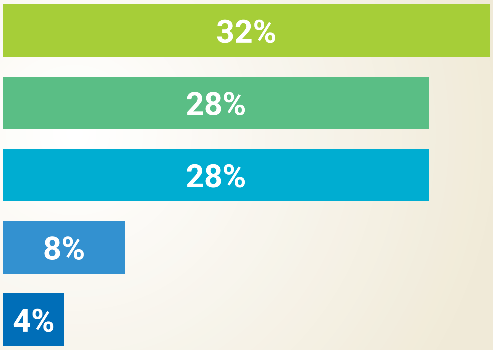


- 🟩 Yes, we have already invested (building it or operational)
- 🟩 Yes, we have decided on the plans (in RFP/vendor selection phase)
- 🟦 Yes, we have a definite mandate but yet to finalize plans
- 🟦 Yes, we are actively exploring
- 🟦 Open to explore
- 🟦 No, no plans in near future

Source: 9.9 Group Research

Objective: Simplifying management of data emerged as the top reason why CIOs want to roll out data lakes, according to our research.

What out of this best describes your reason for going for a data lake?



- 🟩 Simplify management of data
- 🟩 Get insights from data better
- 🟦 Facilitate use of data across co
- 🟦 Save cost
- 🟦 Create a single place for storing data

Source: 9.9 Group Research

Data Lakes in India

In India, the big data lake that State Bank of India—one of the world's largest banks by employees and branches—is building has been in news for some time. SBI listed the following among its key objectives behind building a data lake:

- Application of advanced techniques like Machine Learning within fraud and risk to improve models and allow acceleration towards more real-time analysis and alerting.
- Strong, observable and benchmarked business returns (not just cost take-out) in the broader market.
- To manage explosive growth of data, a solution that will help manage compliance mandates, integrate data governance, etc. "The Data Lake at SBI is expected to serve as a converged regulatory and risk data hub."
- To be able to handle large volume of real time data in possible future IoT based applications.
- Ability to do any analysis at any time ad hoc.
- Optimize total cost of operations for data management, organization, analytics and enable it to streamline data driven decisions.

The five specific areas where it wanted its data lake partner to help were in defining a data lake strategy, defining data lake architecture, benefit realization, defining a path for data lake's evolution, promoting its usage within the bank and in avoiding common pitfalls. Bank of Baroda too came with an RFP for its data lake rollout.

Simplifying data management is key

We decided to probe Indian IT leaders on their stance towards data lakes. We asked them three simple questions:

- What is their current organizational data set-up?
- If they want to go for data lakes?
- If they do, then what is the top driver?

In short, the jury is still out on when and how data lakes would pan out in India. One thing, however, is clear. Indian IT leaders do not buy the skepticism about data centers. They are optimistic ■

GDPR: Privacy Policies Of Online Platforms Have Significant Gaps

BEUC (European Consumer Organization) research suggests AI can help close that gap

The current privacy policies of online platforms and services still have a significant margin for improvement when it comes to meeting the standards put forward by the European General Data Protection Regulations (GDPR), even after more than a month of the regulations kicking in, according to a research by the European Consumer Organization BEUC (or Bureau Européen des Unions de Consommateurs) and researchers from the European University Institute in Florence. The researchers also released a study about how Artificial Intelligence can help scan and analyse privacy policies.

According to a statement by BEUC, none of the 14 online platforms analysed by the researchers came close to meeting the requirements.

"Unsatisfactory treatment of the information requirements; large amounts of sentences employing vague langue; and an alarming number of "problematic" clauses cannot be deemed satisfactory," the organization said.

Google, Facebook (and Instagram), Amazon, Apple, Microsoft, WhatsApp, Twitter, Uber, AirBnB, Booking.com, Skyscanner, Netflix, Steam and Epic Games were the online platforms whose privacy policies were analysed by the researchers.

Based on this analysis, the university researchers are training an automated evaluator of privacy policies, called CLAUDETTE—short for Automated CLAUse DETeCTER. The goal is that this Artificial Intelligence tool will be able to automatically scan companies' privacy policies and detect clauses that potentially fail to meet GDPR requirements.

In total, all the policies amounted to 3,659 sentences (80,398 words). Of these, 401 sentences (11.0%) were marked as containing unclear language, and 1,240 (33.9%) contained "potentially problematic" clauses or clauses providing "insufficient" information.

The identified problems include:

- Not providing all the information which is required under the GDPR's transparency obligations. For example, companies do not always inform users properly regarding the third parties with whom they share or get data from.
- Processing of personal data not happening according to GDPR requirements. For instance, a clause stating that the user agrees to the company's privacy policy by simply using its website.
- Policies are formulated using vague and unclear language—such as "may", "might", "some", "often", and "possible"—which makes it very hard for consumers to understand the actual content of the policy and how their data is used in practice.

> ...the university researchers are training an automated evaluator of privacy policies, called CLAUDETTE —short for Automated ClAUse DETeCTER

BEUC will inform the European Data Protection Board about these findings.

The Method

The CLAUDETTE project has been established in order to attempt automating the legal analysis of terms of service and privacy policies of online platforms and services.

The researchers developed a web crawler that monitors the privacy policies of a list of online services. The data retrieved by the crawler is then processed using supervised machine learning technology. They implemented a Support Vector Machine-based classifier trained on the data set annotated by experts following a set of defined guidelines. Such a data set contains over 3500 sentences taken from 14 privacy policies. The accuracy of the classifier was evaluated using a standard leave-one-document-out procedure, showing encouraging precision/recall in several sub- tasks. The analysis indicates that the task of identifying problematic clauses in this kind of documents is in principle automatable. An extended data set is under construction, whose purpose is to improve the accuracy of the classification results. The expert annotations can be visualized using a standard browser at the CLAUDETTE GDPR web site, http://www.claudette.eu/gdpr/

The web crawler checks for updates in the list of monitored services every night. If any of these services has been updated (i.e., its text appears to be different from the day before), then the machine learning system is automatically called to process the new document, and results are updated on the server.

BEUC is an umbrella consumers group, based in Brussels, Belgium. It brings together 43 European consumer organisations from 32 countries (EU, EEA and applicant countries).

BEUC represents its members and defends the interests of consumers in the decision process of the Institutions of the European Union, acting as the "consumer voice in Europe". The organisation is funded by an EU grant, its member fees and other specific projects.

The full report, CLAUDETTE meets GDPR: Automating the Evaluation of Privacy Policies using Artificial Intelligence, can be accessed in the BEUC website. The report gives a detailed analysis of platforms, some of the clauses where the gaps are and why they are deemed as gaps, based on specific requirements of GDPR.■

Has Tata Motors just taken a step towards the 'platform' future?

By acquiring a stake in a tech-leveraged trucks aggregator, Tata Motors shows that it is willing to invest in learning the rules of the emerging business models

By Shyamanuja Das

Tata Motors recently announced that it has picked up a 26% stake in TruckEasy, a tech-based freight aggregator owned by Loginomics Technologies Solutions Limited, a Bangalore based logistics company.

A 26% stake in a small start-up is a very small incident in the life of a USD 45 billion giant. Yet, this seemingly small step by India's third largest company could well prove to be a giant leap for the large manufacturing companies that want to adjust to the new digital regime.

Be under no confusion. It is not yet another investment in a start-up with promise. The investment was not made by RNT Capital Advisors, Ratan Tata's investment firm. Neither was it done by Tata Sons.

It was, as the company said in its release, a "strategic investment" by Tata Motors, through its wholly owned subsidiary Tata Motors Finance Holdings

> Be under no confusion. It is not just another investment in a startup with promise... It was, as the company says in its release, a "strategic investment" by Tata Motors through its...subsidiary...

Why is it important?

TruckEasy was formed in 2015 in Bengaluru by three entrepreneurs' – Nikhil Thomas, Vikram Kodgi and Avinash Achar. The company provides services for the transporting needs of businesses, using a tech based platform like Uber where users can book the trucks for transportation. At present, it provides its services within Bangalore and one of the stated reasons for this investment is to help it expand its business to other cities within India.

From Tata Motor's point of view, the investment is significant because it points to Tata Motors' acknowledgement of a shift in value creation equation in its business. In a traditional company, value is created upstream and pushed downstream to consumers in a linear fashion. Platform guru Sangeet Paul Choudary calls these companies pipe companies.

But companies like Uber and Airbnb that operate 'platforms' 'allow participants to co-create and exchange value with each other,' explains Choudary, co-author of Platform Revolution: How networked markets are transforming the economy and how to make them work for you and author of Platform Scale: How an emerging business model helps start-ups build large empires with minimum investment

This changes the very design of the business model. While pipes created and pushed value out to consumers, platforms allow external producers and consumers to exchange value with each other.

TruckEasy which brings transporters and businesses together on a tech-enabled Uber-like platform can provide valuable learning to Tata Motors on how the model operates.

Tata Motor acknowledges as much. "This strategic investment in TruckEasy will provide Tata Motors an insight into the rapidly growing technology-driven transformation in the freight logistics space," says the company statement.

"The data analytics provided by TruckEasy will be further used for research and development thereby allowing for better customization of product specifications in line with market requirements," says Tata Motors, in its statement. "We can give deeper insights into the SCV usage pattern with our vehicle data analytics," says Thomas, CEO of TruckEasy.

Data, of course, is the most important component of the platform model. "Data is the new dollar," says Choudary.

There are three value creators in this arrangement. First is, Tata Motor's insights into the dynamics of the logistics industries—the stated objective. Second is, its learning into the new emerging model of interactions-based platform model and finally, the data.

Theoretically, there is another. Tata Motors could scale the platform to get into the logistics game in a bigger way. But that looks a distant possibility. Tatas had got out of the business a couple of years back by selling off their transportation company, Drive India (DIESL).

That does not mean that it would never go back to the business. If it does, the learning from TruckEasy would come in handy. But the present platform of TruckEasy may be too small and too narrowly focused to scale it up.

For the time being, though, both Tata Motors and TruckEasy are willing to talk about only the immediate priorities. "The driver community will be more confident on the aggregation business with Tata's entry," says Thomas. Through this investment from Tata Motors, TruckEasy will be able to access our wide network to grow the supply side and also to expand to multiple locations country wide," says Girish Wagh, President, Commercial Vehicles Business Unit (CVBU), Tata Motors.

This investment may be beginning of a new era for Tata Motors in particular and the logistics and automotive industries in general ■

Hospitality Industry Under Seige From Botnets: Report

Bot-driven credential abuse, DDoS attacks have continued to rise while leveraging new techniques to overwhelm web-facing systems

Cybersecurity defenders face increasing threats from organizations in the form of bot-based credential abuse targeting the hospitality industry and advanced distributed denial of service (DDoS) attacks, according to the Summer 2018 State of the Internet/Security: Web Attack report released by Akamai Technologies. Analysis of current cyberattack trends for the six month period from November 2017 through April 2018 reveals the importance of maintaining agility not only by security teams, but also by developers, network operators and service providers in order to mitigate new threats.

Hospitality Industry vs Bots: Analysis of Fraud Attempts

The use of bots to abuse stolen credentials continues to be a major risk for Internet-driven businesses, but data from this report reveals that the hospitality industry experiences many more credential abuse attacks than other sectors.

Akamai researchers analyzed nearly 112 billion bot requests and 3.9 billion malicious login attempts that targeted sites in this industry including airlines, cruise lines and hotels among others. Nearly 40% of the traffic seen across hotel and travel sites is classified as "impersonators of known browsers", which is a known vector for fraud.

Geographic analysis of attack traffic origination reveals that Russia, China and Indonesia were major sources of credential abuse for the travel industry during the period covered by the report, directing about half of their credential abuse activity at hotels, cruise lines, airlines, and travel sites. Attack traffic origination against the hospitality and travel industry from China and Russia combined was three times the amount of attacks originating in the US.

Geographical analysis of attack traffic reveals that Russia, China and Indonesia were major sources of credential abuse for the travel industry during the period covered by the report

"These countries have historically been large centers for cyberattacks, but the attractiveness of the hospitality industry appears to have made it a significant target for hackers to carry out bot-driven fraud," said Martin McKeay, Senior Security Advocate, Akamai and senior editor of the State of the Internet/Security report.

The Rise of Advanced DDoS Attacks Highlights Need for Security Adaptability

While simple volumetric DDoS attacks continued to be the most common method used to attack organizations globally, other techniques have continued to appear. For this edition of the report, Akamai researchers identified and tracked advanced techniques that show the influence of intelligent, adaptive enemies who change tactics to overcome the defenses in their way.

One of the attacks in the report came from a group that coordinated their attacks over group chats on STEAM and IRC. Rather than using a botnet of devices infected with malware to follow hacker commands, these attacks were carried out by a group of human volunteers. Another notable attack overwhelmed the target's DNS server with bursts lasting several minutes instead of using a sustained attack against the target directly. This added to the difficulty of mitigating the attack due to the sensitivity of DNS servers, which allows outside computers to find them on the Internet. The burst system also increased difficulty by fatiguing the defenders over a long period of time.

"Both of these attack types illustrate how attackers are always adapting to new defenses to carry out their nefarious activities," said McKeay. "These attacks, coupled with the record-breaking 1.35 Tbps memcached attacks from earlier this year, should serve as a not-so-gentle reminder that the security community can never grow complacent."

The key findings from Akamai's Summer 2018 State of the Internet/Security: Web Attack report include:

- Akamai measured a 16% increase in the number of DDoS attacks recorded since last year.
- The largest DDoS attack of the year set a new record at 1.35 Tbps by using the memcached reflector attack.
- Researchers identified a 4% increase in reflection-based DDoS attacks since last year.
- There was a 38% increase in application-layer attacks such as SQL injection or cross-site scripting.
- In April, the Dutch National High Tech Crime Unit took down a malicious DDoS-for-hire website with 136,000 users.■

"Organizations Need To Train Their Employees In Good Operational Security"

Keith Martin, Asia Pacific Head and Corporate Business, F-Secure shares his perspectives on cybersecurity

By ITNEXT

Q Cybersecurity spending is higher than it's ever been – an estimated USD 96 billion this year. Where do you think organizations are investing the most?

A Companies continue to invest the lion's share of their cybersecurity spend in the more "traditional" areas, such as antivirus software, firewalls, and monitoring. However, although the overall percentage is still relatively low, some newer categories, such as endpoint detection and response, as well as vulnerability assessment, are growing at a faster rate than the more traditional types of protection, and we will see them consume an even greater percentage of the spend in the future.

Q Do you finally see organizations turning cybersecurity/security into a strategic asset in the organization?

A Unfortunately, I don't believe this shift in mindset has become very commonplace yet, although it should be. Using the strength of your security as a competitive differentiator can definitely add value to your business and therefore should be seen as contributing to your profit, and not simply viewed as a cost to be minimized.

Q There's a lot going on around cybersecurity and data protection these days, so it's a fantastic set of topics. What are some of the concerns you're hearing from your APAC customers on GDPR?

A There is still a lot of confusion and uncertainty regarding GDPR. Companies really need to clearly understand if this affects their business and, if so, ensure that they have taken the necessary steps to comply with these regulations. GDPR is not only about cybersecurity but also about ensuring that the personal information you have on your systems is sufficiently protected. This is something every company should take seriously, regardless of whether they are impacted by GDPR or not.

Q GDPR will force everyone to raise the bar in terms of security and functionality. How do you think organizations can balance both?

A As our chief research officer Mikko Hypponen has said, "Complexity is the enemy of security." The more complicated we make our systems, the more difficult they are to use and maintain; the more likely they are to be insecure. As an example, one of the data leaks that occurred within the government of Japan happened for exactly this reason. A system that was too cumbersome to use as designed led one user to move data in a spreadsheet to another machine in order to complete their work more efficiently. Unfortunately, that machine was not on the secure network and eventually got compromised. This is a good lesson for ensuring that we don't forget that sometimes the simple solution is both easier to use and more secure at the same time.

Q According to your recent ransomware report, WannaCry is the family behind May 2017's global ransomware pandemic, which is now recognized as the largest ransomware outbreak in history. How can we avoid such attacks from recurring in the future?

A The best way to avoid ransomware is to use reputable antivirus software, preferably one that includes heuristic analysis in addition to a standard signature-based detection engine, and to keep all of your PC software up-to-date with the latest patches and updates. The WannaCry outbreak was enabled by the fact that while there was a Windows patch that would have prevented infection, those 200,000 machines that got infected had not taken the care to keep their systems up-to-date. Finally, be sure to have a backup of your data just in case. If your data is backed up, even in the worst-case scenario of a ransomware infection, you can still restore your data from the backup.

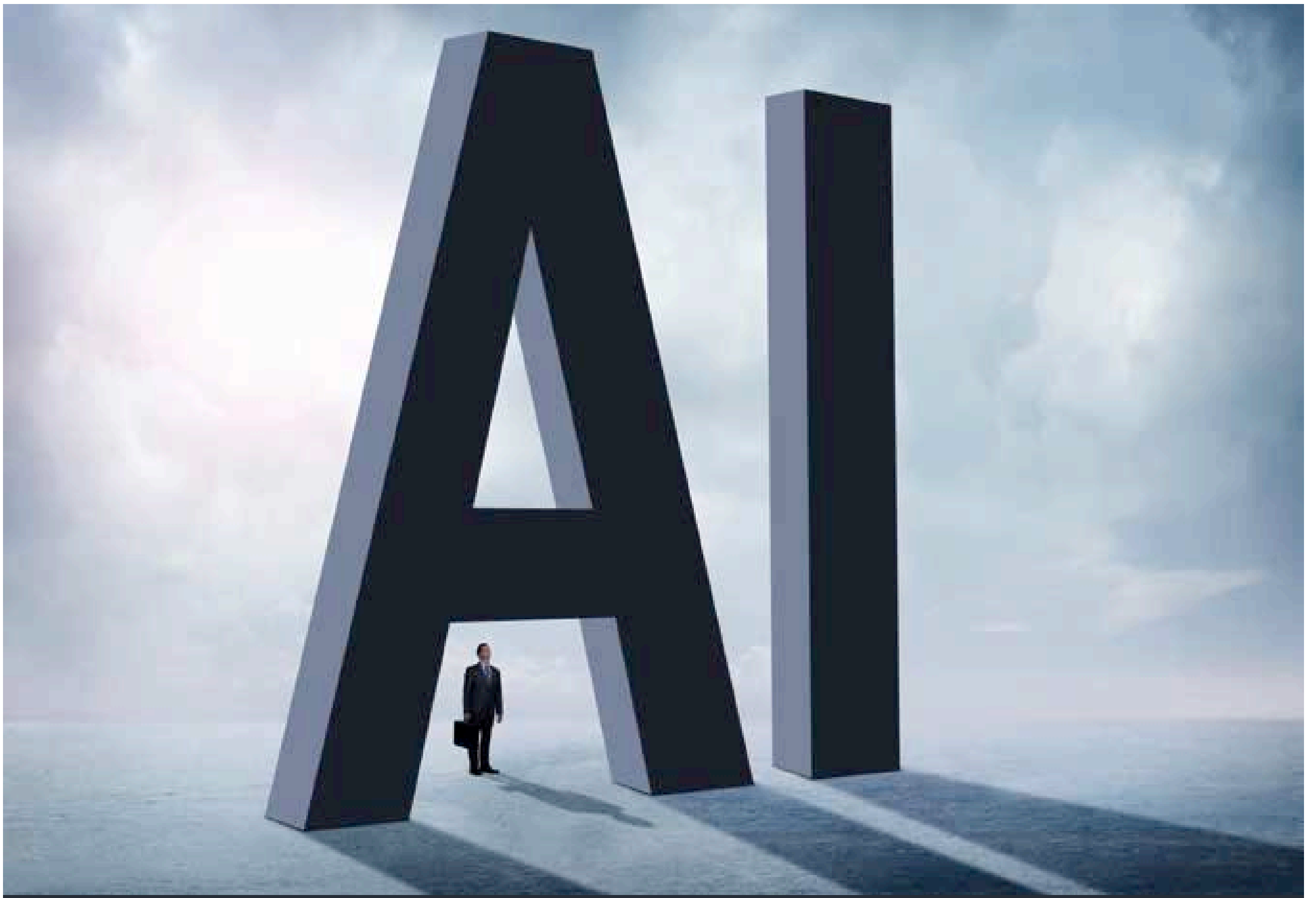
> "The more complicated we make our systems, the more difficult they are to use and maintain; the more likely they are to be insecure...the simple solution is both easier to use and more secure..."
>
> Keith Martin,
> Asia-Pacific Head & Corporate Business, F-Secure

Q What were some of the other important insights that came from F-Secure's Ransomware report?

A One interesting trend is the shift by criminals from ransomware to cryptojacking as a way to make money from their victims. Cryptojacking, rather than encrypting your files and extorting money from you to have them decrypted, involves installing malicious code on your PC that will steal CPU power and bandwidth with which the criminals will mine cryptocurrencies in the background. This trend has been fueled by the recent bubble we are seeing in the value of various virtual currencies, such as Bitcoin, making the mining of coins by using the victim's computer resources an attractive alternative to ransomware.

Q Just about everybody gets endpoint security wrong in one way or another. What best practices do you recommend for CISOs/organizations to ensure that their loose ends are protected?

A Apart from the standard recommendations of ensuring that all systems are fully patched and up-to-date, and using reputable antivirus software on your endpoints, I think it is critical that you train your people in good operational security. Most targeted attacks these days start with a phishing email, which are alarmingly effective at getting an employee to voluntarily divulge their login credentials. F-Secure's own white hat hackers, who regularly do red teaming security assessments, frequently gain a foothold inside the target organization by devising a phishing attack that can easily trick the employees into giving up their login credentials. Using a training solution to provide employees with a greater understanding of the dangers, as well as giving meaningful practice in spotting such attacks goes a long way towards making your company's infrastructure safer ■



India’s Proposed AI Strategy: High On Planning, Low On Ambition

The strategy may, however, give a boost to the industry in the short run

By Shyamanuja Das

The country that leads in artificial intelligence (AI) will rule the world, Russian president Vladimir Putin had famously remarked a few months back. It is no surprise major countries are all formulating their national AI strategies.

While UK, Japan, France, EU and UAE have come out with their AI strategies, Singapore has launched a national program called AI Singapore under the National Research Foundation, a unit of the Prime Minister's Office.

However, it is the Chinese government's three-year development plan for AI, released in July 2017—with more detailed agenda fleshed out in December that year—that has taken the world by storm. Not only has the middle kingdom clear targets about what it wants to achieve—it has not kept its ambition hidden—it is also nothing less than 'to lead the world'. Though US is still way ahead in AI, China has proven in the past that it means what it says and no one is taking its announcement lightly.

India is the latest to join the party. Earlier this month, India's Niti Aayog released a 115-page discussion paper on National Strategy for Artificial Intelligence (#AIforAll).

The industry—including software and services industry association NASSCOM—has welcomed it wholeheartedly.

That is not surprising considering there is a lot in it for the industry. It is a fairly detailed low-level plan. Take, for example, the two-tiered research structure, in which the application oriented research is envisaged to be in partnership with the private industry.

Similarly, there are a lot of initiatives aimed at creating capacity—something the industry badly needs. In fact, addressing the skills gap may be the single-most important fallout of the strategy, if implemented properly.

In addition, the cloud platform that the government plans to set up will also see massive tech investments.

All these—coupled with detailed sectoral application plans—will create immense business opportunity for the industries in the short to medium run. The web of myriad government projects and programs will have a multiplier effect on the industry.

Why India's proposed strategy lacks punch...

Despite getting into so much of detailed planning, the strategy is not a game changer. There's no clear goal; there's no clear positioning either. It has neither the ambition of China nor the will to effectively cope with the socio-economic changes emanating from AI, as planned by EU's AI policy.

Of course, it is a discussion paper and not a policy statement or stated strategy. "The purpose of this paper is to lay the groundwork for evolving the National Strategy for Artificial Intelligence," says Niti Aayog CEO Amitabh Kant in the introduction.

If that is true, it reveals the government's thinking on the approach it wants to take.

Here are the three reasons I think the strategy document lacks punch:

It lacks ambition. Not all ambitions get fulfilled; that does not mean one should not have ambitions. Look at China's policy; while its clear ambition is to 'lead the world', India's AI strategy paper talks of becoming a 'garage' for the developing world. That, by itself, may not be such a bad thing. It will generate enough revenues and keep rolling our body-based services industry.

The strategy is not a game changer. There's no clear goal... It has neither the ambition of China nor the will to effectively cope with the socio-economic changes emanating from AI

But if anything, that is a low-hanging fruit and should tactically be tapped for the short run. Some small government intervention may be required to accelerate that but how can it be a topline goal in a national AI strategy?

Should not we aim for more? Should not we use this opportunity to break away from/disrupt the T&M based IT services and create a completely new opportunity for ourselves? You do not need a major policy intervention for Indian IT services companies to start making money from AI. Availability of skilled people will only accelerate that. But is the goal ambitious enough for a nation like ours?

It lacks clear goals. The entire document has a lot of detailing on what should be 'done'; very little targets about what will be 'achieved'. Apart from 'leading the world', China puts a number to the AI opportunity. In India, there is no target even for specific plans outlined in the strategy document, let alone a big overall target.

There's no result orientation; and that may lead to clear lack of accountability.

It ignores negative social impact aspect completely. This is the most visible exclusion from the policy. As a liberal democracy, India cannot just close its eyes to negative impact of any new technological—or for that matter, any—change.

In European Union's communication on AI for Europe, it is included as one of the three topline objectives—prepare for socio-economic changes

Strategy Paper on AI: Highlights

The framework that the document proposes for developing a long-term national AI strategy has 'three distinct, yet inter-related' components. They are:

- Opportunity: the economic impact of AI for India
- AI for Greater Good: social development and inclusive growth
- AI Garage for 40% of the world: solution provider of choice for the emerging and developing economies (ex-China) across the globe

It then takes a sectoral approach of how AI can create value for sectors like healthcare, agriculure, smart mobllity, retail, manufacturing, energy, smart cities and education & skilling. Five out of these—healthcare, agriculture, education, smart cities & infrastruture and smart mobiliy & transportation—have been identified by Niti Aayog as focus sectors.

Like most national strategies, it has proposed strengthening research, building skills and accelerating adoption as priority sectors. The paper has proposed a two-tiered structure to address India's AI research aspirations—Centre of Research Excellence (CORE) focused on core research in AI and International Centers of Transformational AI (ICTAI) in collaboration with private sector, to take up research on AI applications. Further, it proposes establishment of an umbrella organization, Centre for Studies on Technological Sustainability (CSTS), to address issues relating to 'access to finance, social sustainablity and the global competitiveness of the technologies devetoped.'

It also proposes building a market place, National AI Marketplace (NAIM) for facilitating collaboration, and enhancing access to AI solutions leading to ease of adoption and efficiency. It also proposes a cloud-based AI research, analytics and knowledge assimilation platform (AIRAWAT). Just in case you wonder, Airawat is the name of the mount of Indra, the king of gods, according to Hindu mythology. It is a white elephant.

The document just touches the ethics aspect of AI, mostly dealing with privacy issues. While there is some passing mention of ethical AI, it completely ignores the social impact of AI, even though it is the principle focus of many such policies, such as those of EU and UK.

brought about by AI by encouraging the modernisation of education and training systems, nurturing talent, anticipating changes in the labour market, supporting labour market transitions and adaptation of social protection systems.

While Indian strategy talks of making positive social impact through AI, it completely ignores this aspect—of negative impact on jobs.

Similarly, when it comes to ethics and privacy, there's nothing concrete about ethics in AI research or AI applications. The entire section is almost dedicated to privacy issues.

While a lot of government attention and investment will surely give a fillip to the industry, as a nation, we could realistically aim to achieve more. What is more, without clear objectives, we may just lose the way.

If you do not know where you are going, any road will get you there. ■

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।

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

डिजिट

CFO INDIA

NETWORK

Intelligence . Leadership . Transformation

A PEER-POWERED,
KNOWLEDGE - BASED AND
COMMUNITY-LED INITIATIVE
FOR CFOs

Double Scoop

Two times
the revelation

Neelima Sharma
SAP Lead – Operational Modules
Hindustan Zinc

MY FAVORITE TECH SHOW

IoT and Industry 4.0 shows on YouTube

A CELEBRITY WHO KEEPS INFLUENCING ME

Akshay Kumar

MY FAVORITE SPORT

Kabaddi

MY IDEAL GETAWAY

Kashmir

A TECH BOOK WHICH I'M CURRENTLY READING

SAP S/4 HANA for Manufacturing Excellence

MY PEER IN THE IT COMMUNITY

S Ramaraju
Head - IT, BALCO

MY FAVORITE AUTHOR

Chetan Bhagat

A CUISINE WHICH I LIKE THE MOST

South Indian

A TECH EVENT WHICH I ATTENDED RECENTLY

Digitization Workshop

A GADGET WHICH I CAN'T DO WITHOUT

Smartphone

MY PASSION

Sports

Street lamps will know day from night
Making Businesses #SmarterWithIoT
Global leader in IoT
O&M 2871
The future is exciting.
Ready?
vodafone