

India in the Security Hub

Is Artificial Intelligence Shaping the Future of ERP Software

₹125

VOL. 32 | ISSUE 9 | SEPTEMBER 2019

PCQUEST

UNDERSTAND • CHOOSE • IMPLEMENT IT

TECH TALK

Digital Disruption, AI and IoT in CRM

— Colleen Berube
CIO, Zendesk



BEATING THE HACKERS

The cybersecurity war has just begun

INDIA'S
NO.1*

PC BRAND

*As per IDC CY Q2 2019 market report.

Available with
PREMIER SUPPORT

WHAT'S THE WORST THAT CAN HAPPEN TO A THINKCENTRE? **NOTHING.**

Lenovo

M720 SFF

M720 TOWER

M720 TINY

M90 NANO

Introducing ThinkCentre. The most versatile range of desktops you can get your hands on. You may run a small business, a start-up, or a massive enterprise, a ThinkCentre will work without fail in any workplace. Because every ThinkCentre, from a Nano to a Tower, is built to withstand the most complex of tasks in the harshest of work environments.

ThinkCentre

Starts at ₹26,900.**



200 Quality Checks



Military-spec Tested



Dust and Humidity Shield



Handles Extreme Temperatures



Powered with Intel® Core™ i7 vPro™ processor

Windows 10

Windows 10 Pro means business.

1800 102 5296 | corpsales@lenovo.com | www.lenovo.com

Lenovo reserves the right to alter product offerings and specifications at any time without notice. Models pictured are for illustration purposes only. Lenovo is not responsible for photographic or typographic errors. Information advertised has no contractual effect. Lenovo, the Lenovo logo and ThinkCentre are trademarks or registered trademarks of Lenovo. © Lenovo 2019. All rights reserved. **Terms and conditions apply. Talk to your nearest dealer for offer details.

Bible of Indian ICT Industry

Volume 1 will emphasize on all the traditional means, which serves as the backbone of the entire ecosystem, i.e Infrastructure

Volume 2 will focus on all the new & futuristic technologies, which will serve as the backbone of the modern Industrial revolution.

Infrastructure

Hardware



PC

Server

Storage

Networking



Peripherals

Datacentres

Hyperconverged Infrastructure



Operating System

Office 365

CRM

ERP

Software



SCM

Information Management

Storage

BI

Services



Outsourcing

AMC

Volume 2: Emerging Technologies



Artificial Intelligence

Machine Learning

Deep Learning

Blockchain



Augmented Reality

Internet of Things

Industrial Internet of Things

Virtual Reality



Mixed Reality

Edge Computing

Quantum Computing

Robotic Process Automation



Cloud

Security

Special Section

Association Options

- Advertisement
- Magazine Cover Wrap
- Book-Mark
- Customised Envelope

- Cover on Cover
- Specialised Mailing
- Section Sponsorship
- Flap Cover

- Custom Copies
- Content Marketing
- Social Media

Connect with Dataquest for 360 degrees marketing program
for year long brand engagement

For Strategic Partnership and Advertising Opportunities

Rajiv Pathak: rajivp@cybermedia.co.in, Tel: 0124 482 2222 ext: 219, M: +91 8010757100



AMD - High Performance Computing and Graphics Leader



VINAY SINHA

Managing Director, Sales
AMD India Private Limited

At AMD, we are on a mission to become a high-performance computing and graphics leader. To accomplish this, AMD has returned to what it does best – building high-performance products. We are focused on establishing long-term leadership across the \$75B high-performance computing and graphics market [globally], which includes a \$29B datacenter opportunity across CPU and GPU. Customers are betting multi-million-dollar parts of their businesses on AMD based on the strength of our current product portfolio, long-term roadmaps and consistent execution.

We are proud of the progress we have made with our “Zen”-based high - performance EPYC™ processors, Radeon™ graphics and Ryzen™ processors.

- We have gained steady momentum with our Ryzen™ and EPYC™ processors delivering seven straight quarters of year-over-year x86 market share gains, demonstrated by Mercury Research x86 market worldwide share estimates for Q2 2019.

- We are working with some of the biggest names in the datacenter industry. The top 5 server OEMs (Cisco, Dell, HPE, Lenovo, Supermicro) and six of the “Super 7” mega-datacenter providers (Google, Microsoft Azure, AWS, Baidu, Alibaba, Tencent) are all using EPYC™ CPUs and/or Radeon™ GPUs in their datacenters.

- Future generation AMD EPYC™ CPUs and Radeon Instinct GPUs were selected to power what is expected to be the world's fastest supercomputer when it is delivered. The Frontier system is expected to achieve more than 1.5 exaflops of processing power.

Our next major milestone is the introduction of a complete 7nm product portfolio, a major step for the company and a noteworthy time in the industry as we outpace our competition in the most cutting-edge process node for the first time ever.

- 7nm Ryzen™ desktop processors and Radeon™ graphics products for gamers, creators, enthusiasts and the datacenter are now available in market.

- On August 7, we launched the world's first high-performance x86 7nm server CPUs, our next-generation EPYC™ processor (codenamed “Rome”) based on the “Zen 2” CPU core.

This year AMD is celebrating 50 years of innovation in the semiconductor industry. We are committed to bringing increasingly more computing and graphics power to a larger part of the world's population so that the best and brightest have access to the tools they need to solve some of the world's biggest challenges.





Celebrating 50 Years of Innovation

AMD designs, integrates and evolves high-performance computing and graphics technology to solve some of the world's toughest and most interesting challenges.



A NEW BREED OF PROCESSOR

New AMD PRO Processors for business.
The professional grade security and manageability you need,
the experience you deserve.



Contents

12-35 COVER STORY

P12 WITH THE RISE OF DIGITISATION, THE WORST IS YET TO COME



Jyoti Prakash is Country Director of Enterprise Security Business, Micro Focus India. He says that at least 4 billion records, including credit card numbers, home addresses, phone numbers and other highly sensitive information, have been exposed through data breaches in 2019



P15 In Vogue: White Hats

**P19 ML Technology To Secure
Card Transactions**

**P21 Security-Scape From A Global
Analyst**

P23 Security Perils In Retail Sector

P25 Lagging Areas

P26 Major Security Breaches in 2019

P28 Security Threats In Numbers....

**P30 Why Blockchain Matters In
Cybersecurity And In Open Internet**

**P33 Making India "Man-in-the-Middle"
Attack Free**

**P35 Network Security & Cyber Risk
Management In India 2019-2014**

SEPTEMBER 2019

IN CHARTS

36 Global DNS Threat In 2019

39 India In The Security Hub

FOCUS AI

40 AI Can Pave The Way For More Impactful Digital Business Models



FOCUS AI

42 Is Artificial Intelligence Shaping The Future of ERP Software



44 Conversation Gateways: The Holy Grail of Customer Experience Management

46 Adopting AI: How To Ensure Smooth Implementation

48 AI Making Breakthroughs In Indian Banking And Healthcare

50 Why The Time Is right For AI ML Business

GADGETS CORNER

54 Techno Phantom 9 Review



55 Crossloop Designer Pro Series Earphone Review



TECH TALK / TECH MIRROR

58 Understanding The Ink Tank Printer Revolution

62 IoT And Smart Home Have Multiple Applications In The Indian Market

65 Digital Disruption, AI And IoT In CRM

68 There is A Great Shift From Multichannel To Omnichannel

70 Are Companies Hiring Software Engineers All Wrong?

LAST WORD

73 Why India's Manufacturing Sector Needs

SUBSCRIBE NOW!



Turn to page 60

GO AHEAD AND TOTAL UP ALL THE PEOPLE WHO LIVE IN BAHRAIN, QATAR, AND OMAN.

YOU NOW KNOW THE MILLIONS OF READERS MAGAZINES HAVE ADDED SINCE 2017.

The math is simple. You are looking at almost 90 lakh new magazine readers in India. (85.90 lakhs to be precise.) Or a gain of around 9 million readers across the last 2 years. Considering this is part of the new IRS (Q1 IRS 2019), you now have millions of reasons to reinforce your magazine plan. With 63% of magazine-reading India younger than 30, your media plan can now reach an even bigger chunk of an India that's eager to buy. Who knows by next year, we might have to use very different comparisons to give scale to our numbers.

MAGAZINES ☐ REACH
☐ ENGAGE
☐ CONNECT

(SOURCE: Q1 IRS 2019. COMPARISON: WITH IRS 2017.)





Association of Indian Magazines



banginthenmiddle

EDITORIAL

CONSULTING GROUP EDITOR: Ibrahim Ahmad
MANAGING EDITOR: Thomas George
EXECUTIVE EDITOR: Sunil Rajguru
ASSOCIATE EDITOR: Soma Tah
ASSISTANT EDITOR: Archana Verma, Supriya Rao
CONSULTING EDITOR: Anusha Ashwin
ASSISTANT EDITOR (Special Projects): Ankit Parashar
CORRESPONDENT: Aanchal Ghatak
DESIGN MANAGER: Nadeem Anees

VICE PRESIDENT RESEARCH: ANIL CHOPRA

CYBERMEDIA LABS

MANAGER LAB: Ashok Pandey

BUSINESS

SR. VICE PRESIDENT: Rachna Garga (rachnag@cybermedia.co.in)

NORTH:

ASSOCIATE VICE PRESIDENT: Harminder Singh
MANAGER: Sudhir Kumar Arora, Mohammad Shoeb Khan

SOUTH:

GM: Rajeeb Banerjee
MANAGER: Shubhadeep Sen

WEST:

GM: Rajeeb Banerjee

MARKETING & ALLIANCES (marketing@cybermedia.co.in)

SR. VICE PRESIDENT: Rachna Garga
ASST. MANAGER MARKETING: Rajiv Pathak
MANAGER, MIS & DATABASE: Ravi Kant Kumar

OPERATIONS

GENERAL MANAGER: CP Kalra
MANAGER: Ashok K

EVENTS & COMMUNITIES

SENIOR MANAGER: Debabrata T Joshi
ASST. MANAGER: Shiv Kumar

CIRCULATION & SUBSCRIPTIONS

HEAD: Rachna Garga
SR. MANAGER: Sarita Shridhar
SR. PRESS CO-ORDINATOR: Harak Singh Ramola
CHENNAI: C Ramachandran

For subscription queries contact: rsepcg@cybermedia.co.in
Send all your tech questions to: pcquest@cybermedia.co.in

CORPORATE OFFICE

Cyber House, B-35, Sec-32, Gurugram (NCR Delhi) 122001. India
email us pcquest@cybermedia.co.in
call us +91-124-482-2222, **fax us** +91-124-238-0694

OUR OFFICES

BENGALURU

Address: 205-207, Sree Complex (Opp. RBANMS Ground)
73, St John's Road, Bengaluru - 560 042
Tel: +91 (80) 4341 2000, Fax: +91 (80) 2350 7971

MUMBAI

Address: 404 Trade Square, Mehra Industries Compound Safed Pool,
Sakinaka, Andheri East, Mumbai - 400072
Mobile: 9969424024

DELHI

Address: Cyber House, B-35, Sec 32, Gurugram,
NCR Delhi-122001. Tel: 0124-4822222, Fax: 2380694

USA

Media Representative: Ms. Leslie Hallanan, Avani Media Inc.,
80 Liberty Ship Way, Suite 25, Sausalito, CA 94965, USA
Tel: +1-415-3312150, Fax: +1-415-3312151
Email: info@avanimedia.com, Website: www.avanimedia.com

Printed and published by Pradeep Gupta on behalf of CyberMedia (India) Ltd, printed at printed at M/s Karan Printers, F 29/2, Phase II, Okhla Industrial Area, New Delhi, published from D-74, Panchsheel Enclave, New Delhi-110017. Editor: Anil Chopra. Distributed in India by IBH Books & Magazines Dist. Pvt. Ltd, Mumbai. All rights reserved. No part of this publication may be reproduced by any means without prior permission.



www.pcquest.com



http://twitter.com/pcquest



http://facebook.com/pcquest



http://linkd.in/pcquest



http://gplus.to/pcquest



pcquest@cybermedia.co.in



Sunil Rajguru, Executive Editor
sunilr@cybermedia.co.in

The Perils of 100% Digitisation

The Industrial Revolution has been retroactively called Industry 1.0. After that the telegraph and railroad transformed society with the fast dissemination of goods, people and mainly ideas. We called that era Industry 2.0. After World War II came a period of great technological progress with the PC and Internet revolutions. That's Industry 3.0 in which we are still in.

The period to come has been dubbed Industry 4.0: Smart homes, smart cities and smart manufacturing powered by the all-pervasive Internet of Things (IoT). That and dark factories which won't even require people to monitor them and will be able to function remotely 24x7.

All this to be ably aided by the ongoing mobile and GPS revolutions. Then there's the alphabet soup of Artificial Intelligence (AI), Machine Learning (ML) and Robotic Process Automation (RPA). In business Digital Transformation is the new mantra and in things like Hyper-Converged Infrastructure (HCI) everything is virtualised.

On the personal front, the mobile is the be all and end all and you don't need anything else. It is your best friend, social media circle, camera, messenger and it helps you hail a cab, know where you are and order virtually everything under the sun. Welcome to the world of 100% digitisation, which escaped Industries 1-3.0 but is inevitable in Industry 4.0.

The machines and hardware are fading totally into the background and the duo of software and data are firmly in the foreground. In fact an exciting (or scary depending on how you look at it) proposal is Billionaire maverick genius Elon Musk's Neuralink. Electrodes will be connected to your brain which will link to a device embedded under your ear which will control computers. That takes the other HCI (Human Computer Interface) to a totally new level.

But if everything is virtualised and everything is connected, then everything can be hacked, attacked and manipulated. Cybersecurity will no longer be about viruses that can bring down a system and the theft of data. The whole world will be one interconnected cyber organism encompassing the Internet, the Internet of People and the Internet of Things. Hollywood film Terminator's Cyberdyne Systems doesn't seem that far away in the 2020s.

Aadhaar became the first system in the world to get the biometrics of more than a billion on its database, which is currently ruling over all of our documentation. China upped that and took it to a different level with dynamic real-time facial recognition. Together a clear 2.5 billion+ are on these systems. Is it all safe?

In the future Cybersecurity will probably be the single most pressing issue facing mankind.

“
**The duo of
software and data
are firmly in the
foreground**
”

Sunil Rajguru

WITH THE RISE OF DIGITISATION, THE WORST IS YET TO COME

Jyoti Prakash is Country Director of Enterprise Security Business, Micro Focus India. He says that at least 4 billion records, including credit card numbers, home addresses, phone numbers and other highly sensitive information, have been exposed through data breaches in 2019

Sunil Rajguru
sunilr@cybermedia.co.in



Has 2019 been a bad year for cyber security?

Data breaches have gained a lot of attention owing to the rapid evolution of digitisation. Businesses of all size, nowadays, have become increasingly dependent on digital data, cloud computing and workforce mobility. With data being stored on machines, database and servers, invading a company's data has

become simple.

Whether it is the recent Poshmark breach, Capital One breach, Bulgaria's National Revenue Agency breach, NASA breach or Facebook breach, millions and millions of users have been affected worldwide. If you look at it, on an average, every 10th day of the month you see another breach happening across

every corner of the globe.

Given the rise of digitisation, we feel that the worst is yet to come. We will see an increase in targeted ransomware attacks – criminal groups continue to target businesses, banking, health care providers, and, most visibly, local governments with these brash hacks. At least 4 billion records, including credit card numbers, home addresses, phone numbers and other highly sensitive information, have been exposed through data breaches in 2019.

According to a recent report revealed by EY, more than three-quarters (87%) of organisations do not yet have a sufficient budget to provide the levels of cybersecurity and resilience they want, a reason why data thefts are happening. In India, we feel that 2019 will be a challenging year for security professionals. These new threats and challenges prevailing in the country will incite professionals to think differently in order to address the same.

Going forward, companies need to ensure that sufficient budget is provided to help overcome the growing concerns of cybersecurity. Additionally, they will have to invest in upskilling their security professionals so that they can get ready to address and respond to known, unknown threats. While this year has seen a lot of cyber-attacks, we are confident that companies will come up with more features and solutions that will help reduce such incidences.

What are the further threats we can expect as digital transformation cases are on the rise?

The advent of immersive technologies is causing firms to reimagine traditional business models and innovate new ways to leverage data for growth. According to a recent IDC research, two-thirds of the CEOs of Global 2,000 companies will shift their focus from traditional (offline) to modern (digital) strategies in order to improve customer experience, before the end of 2019 – with 34% of companies believing that



JYOTI PRAKASH
Country Director, Enterprise Security Business
Micro Focus India

they will fully transform themselves digitally within 12 months or less.

As threat landscape continues to evolve, companies need to adjust their strategies. There is a tremendous value with having the right combination of technology products and processes in the digital transformation journey. An agile enterprise can thus, help act rapidly and react to changing data, competitive conditions and strategies to succeed and

guard against disruption. Additionally, DevSecOps is going to lead this transformation journey, as applications are becoming business drivers. They are also becoming more prone to targets. We feel that a wholesome security strategy, embedded in each stage of application development cycle, would be the right move ahead.

If we look at 2019, half of the year is already on the books and there have certainly been data breaches, supply chain manipulations, state-backed hacking campaigns, cyberwar, etc. to show for it

What will be the dangers in Industrial IoT (Industry 4.0)?

Industry 4.0 or the increased connectivity of smart machinery indicates a new age of connected, smart manufacturing, responsive supply networks, and tailored products and services. It strives to marry the digital world with physical action to drive smart factories and enable advanced manufacturing. While Industry 4.0 plans to enhance digital capabilities, it will also bring new cyber threats, for which the industry is still not prepared.

Will AI-ML make our systems safer or will they lead to their own host of problems?

As we are going ahead with the fast-paced digital environment, we see a drastic rise in data volume – this leads to a requirement for a strong cyber breach defence framework. We need to implement a holistic security framework to identify, protect, detect, respond and recover from cybersecurity threats – AI & Analytics can help only if it is implemented in the right manner. Acquiring data from historical threads and baselining the same is of utmost importance in order to detect threats properly and efficiently. This will in turn, help reduce millions of threat incidences into limited “Threat leads” and AI framework will play a critical role here.

What exactly is a Security Operations Centre (SOC) and why should enterprises invest in it?

SOC has a single co-relation engine, along with a single dashboard, which collects lots of technologies and gives a holistic and real-time view to any end customer. In fact, it is a journey that one needs to take and even if one invests in a SOC, it is pertinent to figure out whether the SOC is functioning efficiently or not. With an integration of SOC with multiple products – coming from multiple sources, real-time analysis that one gets, visibility that one has, compliance level and policy that needs to be enforced, are the trigger points that define the efficiency of a SOC. So, any organisation who has already invested in a SOC will be able to identify if there’s any data breach that is happening or is about to happen. This is the reason why SOC came into the market and over time, it has become much more intelligent.

Are CIOs/CTOs able to keep up with the above-mentioned threats and what more do they have to do to keep their enterprises safe?

CIOs/CTOs need to spend time and effort to reduce business friction, minimise wasted time and resources. They should work together to minimise the historical tension between IT and rest of the organisation. CIOs/CTOs, as leaders, need to increasingly teach others how to respond to coming transformation and be adept at selecting the most efficient IT platform and employing agile, lean development practices. Additionally, they need to take out time to train their IT professionals on company’s business culture and customer expectations, for a better and safe enterprise.

Is cyber insurance necessary and what kind of insurance should be done?

With digital transformation on the rise, security concerns have also risen. Today, majority of us use smartphones/laptops and carry out financial transac-

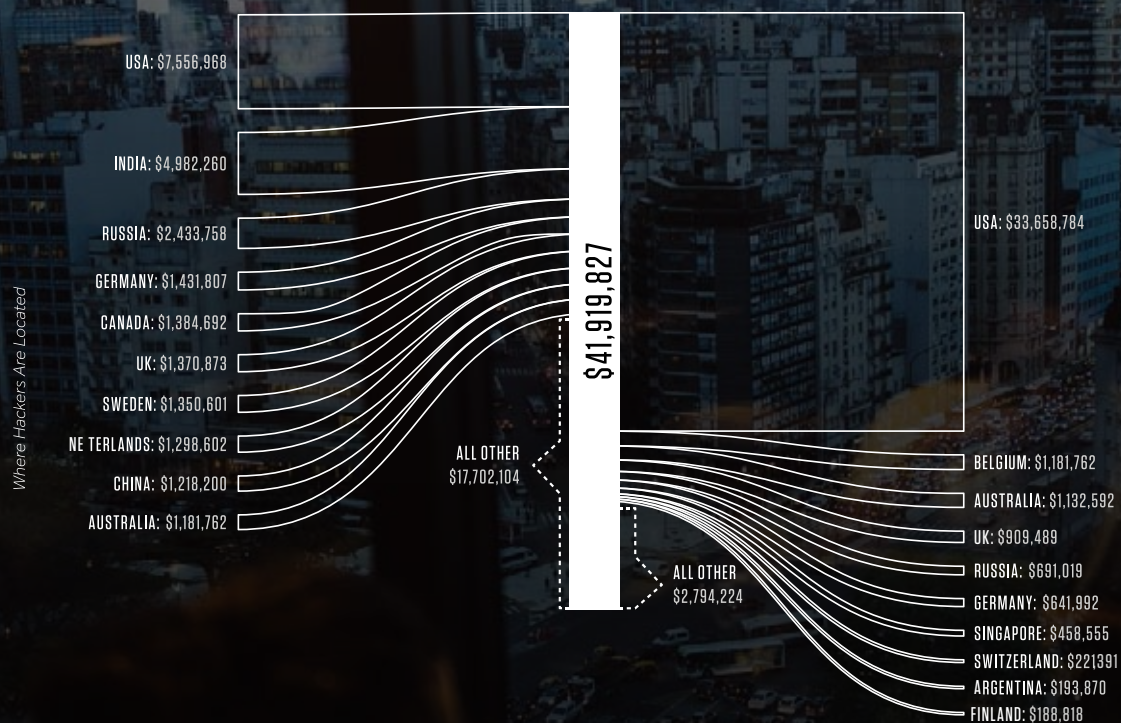
While digital transformation is altering security needs in some fundamental ways, here are some of the changes that we should be aware of:

- * **Expanded attack surface** - As more and more applications, data and processes move into the digital realm, hackers will get more opportunities to invade.
- * **Damage can be high** - Given the dependency of organisations on digital technologies, an attack can be more damaging for them.
- * **Uncontained enterprise networks** - Most companies use some kind of digital applications and may host their servers in the cloud. It means the company networks are not contained and have connections to the publicly accessible internet. This can help hackers access the company networks and ruin their infrastructure.
- * **Rapid change** - The increased speed of technological advancements makes it easier for security vulnerabilities to slip through. Since cybercriminals are coming up with advanced ways of hacking, security professionals need to work constantly to come up with new ways of protection.
- * **Increased sophistication of attacks** - Technological advancements have made cybercriminals more sophisticated in nature. While an AI solution is a welcome boon for companies, it is also aiding cybercriminals.

tions not just from our personal gadgets, but also from office computers and public internet connections. Accessing personal information from various devices, hence, exposes us to different types of connectivity risks. It is, hence, imperative for us to secure data.

While cyber insurance cannot stop cybercrime from happening, it can help maintain/stabilise a business’ financial structure, should a significant security event occur. Any organisation that collects, stores and maintains customer data or facilitates and stores online transaction data, or uses cloud, should ensure adding cyber insurance to its budget. This will help save organisations from huge business loss in terms of financials.

GEOGRAPHIC MONEY FLOW



Visualization of the Bounties by Geography showing on the right where the organizations paying bounties are located and on the left where hackers receiving bounties are located.

Image Source: HackerOne, The 2019 Hacker Report



Hackers were once a mystery. As organisations begin to understand what hacking is, our perceptions change from fear to understanding.”
–Laurie Mercer, Security Engineer, HackerOne

to ascertain their preparedness for a security attack and how resilient they are. This also provides them inputs for improving their security monitoring capability,” said Vishal Jain, Partner, Deloitte India. This works on a pretty basic logic: ‘To catch a hacker you must think like a hacker’. “For consultants like us, we help our clients pre-empt threat situations by the way of Ethical Hacking. At our Deloitte Cyber Intelligence Centre, for instance, the ethical hackers are putting themselves in the shoes of the hackers to show an organisation where their weaknesses lie.”

“There are young independent security professionals who closely watch the activities from the hackers’ perspectives and publish or provide inputs to different agencies/enterprises from the security perspective, including government bodies where they are engaged. These activities are sensitive to national security, hence not disclosed to public generally,” he added.

Laurie Mercer, Security Engineer at HackerOne said, “At HackerOne we see thousands of Hackers helping organisations prevent data and security breaches every day. Governments also continue to lead the way with their successful hacker-powered programmes. The US Department of Defense has partnered with HackerOne for several years, running pioneering programmes such as Hack the Pentagon and Hack the Army to great success. The European Commission partners with HackerOne as part of a framework created by the EU-Free and Open Source Software Auditing (EU-FOSSA) project, which aims to help EU institutions better protect their critical software.”

Bug Bounty

It may sound crazy, but organisations, as part of the vulnerability management strategy do pay out an insane amount of money as bug bounties to the security researchers and the ethical hackers every year. In the recently concluded Black Hat 2019 conference in the US, Apple announced opening



“Industry estimates say that India will need 5 lakh cybersecurity professionals by 2020. We have only 50 thousands of good hackers or white hat hackers. The skill deficit is quite clear.”

–Sandeep Sengupta, Founder & Director - Indian School of Ethical Hacking

up of its bug bounty programme to all researchers and sweetened the payouts by increasing it from the current \$200,000 to \$1 million. Microsoft also announced that it will add a \$300,000 award to its Azure bounty programme to hack its public-cloud infrastructure service. Facebook’s bug bounty programme has paid out more than \$7.5 million since its inception in 2011 and has also paid its biggest single bounty ever- \$50,000, to one of its top contributors. Google’s Vulnerability Rewards Programme dates back to 2010 and has since paid out more than \$15 million. The largest single payout was \$41,000.

Ethical Hacking and India

The bug-bounty platform, HackerOne’s 2019 report says that it paid out over \$42 million to the 300,000 hackers in its network alone, for reporting over 100,000 vulnerabilities. While, most of these bounties came from the US and Canada based organisations followed by the UK, Germany, Russia, and Singapore, etc. it’s an interesting fact that hackers from India continued to dominate the earnings scene by pulling in close to 12 percent of the total bounties paid, and remain the top hacker location too.

According to Mercer, “Over 10 percent of the HackerOne community is located in India. Of the 42 million dollars paid to hackers, nearly 5 million has been paid to India. Top Indian hackers have been paid hundreds of thousands of dollars.” Recognising the strong talent base, HackerOne now supports payments in Indian currency as well to cut down on the unnecessary fees and make the payout process hassle-free for the deserving hackers.

Although financial incentives attract a lot of bug bounty hunters, there’s more to hacking than money. The motivation could be self-serving, or altruistic, or even a mix of both. Some do it purely for fun or for an adrenaline rush, which they get by outsmarting others.



“Enterprises or security services companies do prefer professionals who have the mindset of hacking, provided they are matured enough to use their skills in a constructive manner and for the benefit of the enterprises.”

**–Vishal Jain, Partner,
Deloitte India**

Some do it to hone their skills, while some do it to protect others and to do good for all.

Ethical Hacking Career

With companies hiring from within the hacker community, many are trying to build an effective career plan out of their interest and hacking skills. Conservative estimates say that an ethical hacker generally starts with a Rs 3.5 lakh per year salary, depending on the education, experience and the employer. “Good hacking skills would be a cherry on the icing for a company who is looking at hiring an individual for a cybersecurity role,” said VeditBaxi, Co-Founder and Lead ECS, Lucideus, a leading Indian cyber-security startup.

Depending on the expertise, ethical hackers get hired for a bunch of job roles such as Information Security Analyst, Security Analyst, Security Consultant, (Computing / Networking / Information Technology), Penetration Tester etc.

Many hackers are self-taught. There are no hard and fast rules to follow for anyone aspiring to be an ethical hacker. Usually, a bachelor's degree in computer science and a fair understanding of operating systems, databases and networking with programming skills are good to start. Adding certifications like CCNA, CISSP, CEH, GPEN, CPTC, CPTe, OSCP, Foundstone Ultimate Hacking, etc. can certainly beef up your resume, and increase your chances of getting noticed by the prospective employers, but you need hands-on experience also to back those certifications up. Participating in bug bounty programmes is a great way to test and demonstrate your skills.

“If you are a programmer, you need to have the knowledge of OWASP (secure coding), so the application you make doesn't get hacked. Similarly,



“A hacker needs to know the technology they are dealing with inside out. Thus, it's the hunger to know what keeps them driving, thereby making this digital tech world secure.”

**–Rahul Tyagi, Co-
Founder & VP, Lucideus**



“The way I see it, it's never-ending learning that motivates a hacker. When you keep learning, you end up creating a strong position for yourself in any organisation that you are a part of.

Financial compensations are an eventual benefit of the on-ground work that you would be doing.”

**– VeditBaxi, Co-Founder & Lead ECS,
Lucideus**

network security needs the knowledge of CCNA and software security needs the knowledge of Java, HTML, SQL,” said Sandeep Sengupta, Founder and Director, Indian School of Ethical Hacking.

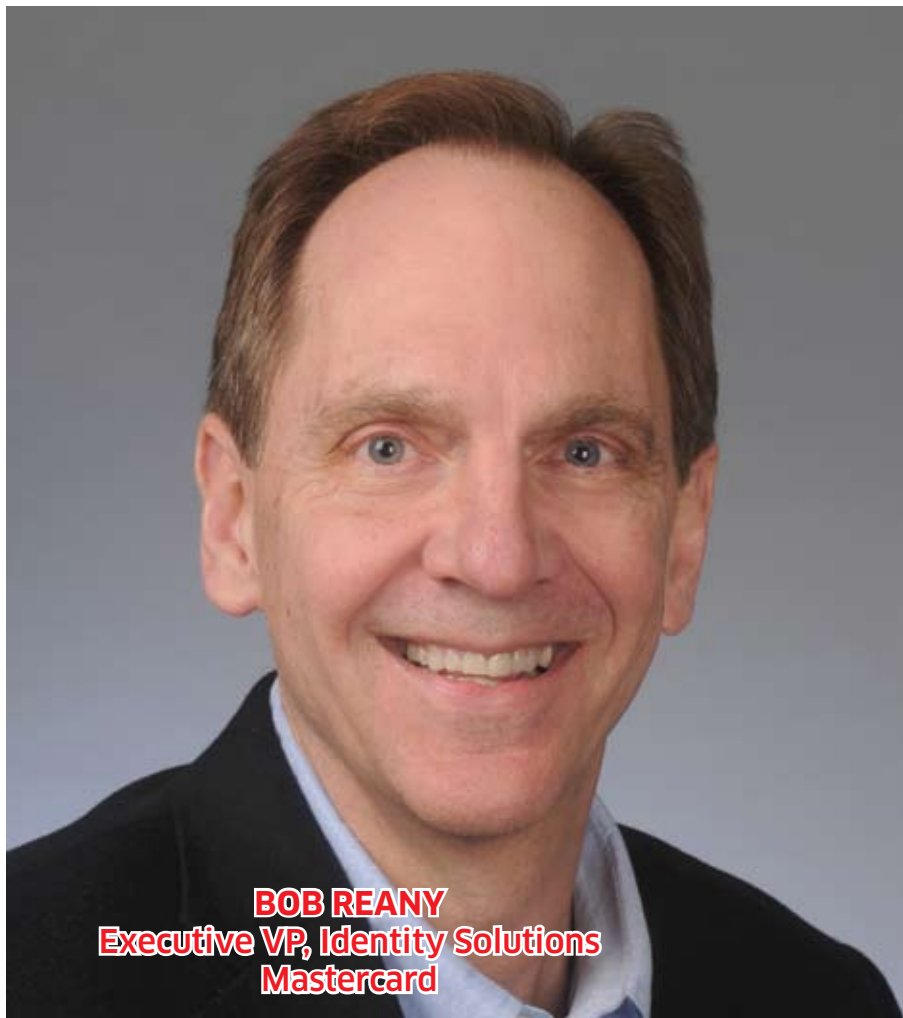
But the career advancement in this domain is dependent on proving your value at work. Creating a habit of self-learning is extremely important in this field to ensure that you are on top of the latest vulnerabilities and security trends. “An individual can have good hacking skills only if their understanding of technology is appropriate. And a technology enthusiast will always focus on learning and growth. Depending on the hunger for learning, you would see people investing time in self-learning and investing money in learning programmes,” said Baxi.

Cybersecurity is an evolving field and presents great opportunities ahead for the ethical hackers. The skills, certifications, and ethics are key for anyone looking to build a successful career, but you also need to be a self-motivated individual with a problem-solving mind, who can assess risks and think of resilient strategies to protect organisations against any cyber-attacks or breach.

ML TECHNOLOGY TO SECURE CARD TRANSACTIONS

Mastercard has come up with a multi-layered authentication system to secure online transactions. This system uses ML to validate the authentication credentials. Bob Reany, Executive VP, Identity Solutions, Mastercard discusses the various aspects of this technology

Dr Archana Verma
archanav@cybermedia.co.in



BOB REANY
Executive VP, Identity Solutions
Mastercard

Is this multi-authentication system like Google Pay?

No, it's a little different in the sense that our job is to connect consumers to merchants to bank. Google Pay is a connect between Google and the merchant. Some of the mechanisms are similar, but my job is to see that the data flows through the bank. They're ultimately responsible for the card that they give you. It may look the same to the consumer but the technology behind the scene that sends information to the bank is very different.

Google Pay allows us to have several layers of authentication with all cards. So, if I link Mastercard to Google Pay, then why do I need this authentication mechanism?

They're not showing the information to the bank. The bank gets only a stripped-down message saying that



you bought something at some place. It doesn't tell you about the geo-location, the device ID, whether it's validated through fingerprint and face recognition etc. when you don't use ML to send all this information, you allow cracks in the system.

Can you explain this technology in some detail?

The bank doesn't get much information when you make a digital payment. So, it sends an OTP which is a very stripped-down method of authentication. This system is doing a lot more. When I want to buy something, I type my PIN. This is validated on my phone itself. It's not shared on the network, no one can see it. We use the term cryptogram which analyses how the algorithm works. It's a mathematical proof that the device is the device that I'm expecting; and the PIN has been validated and the proof goes through a flow and it goes into ML algorithm. The ML looks at the proof from the device and it looks at the data that comes with it like the geo-location, the consumer's app, the device ID itself, it will look at the analytics, at the behavioural parameters which help make it a decision. It uses high security standards.

How many levels of authentications are there?

There are 200 pieces of data and there are 5 or 6 levels of authentication. It checks all your parameters and validates them, so it's more secure than the OTP.

Suppose I buy a new phone and I'm travelling

Then you may have to do an OTP in that case.

So ultimately, I have to use the OTP system

I wouldn't say that. If we can eliminate it 98% of the times then we have done quite well. So in those times you may have to call your bank. Normally it should be hard. I don't want it normally to be easy because if it's a fraudster, then it will be a problem. So if you get a phone, you validate it with your bank and re-write the credentials and now it's ready to go. And then I can use that phone a thousand times and it's going to be quite easy. First time it will be hard and we want it to be hard because we don't want people to misuse your credentials. We have to validate you, so that you can use it multiple times without any problem. It's a much better model than the challenge of getting the OTP every time you use it. You can Google OTP cracked by the users, There are many hackers who can crack the OTP and misuse your data. OTP can be redirected, OTP can be read, OTP can be given away, OTPs are past their prime. Fraudsters know how to misuse OTPs. We've invested millions and millions of Dollars on technology to make it safer. Everything has a generation of beginning and an end and OTP is towards the end. The US and Europe standards of technology have phased out OTP as a two-layers of validation.

5G and IoT won't work with the OTP system. Our multi-factor validation plumbs information about millions of merchants. It gives good customer experience and authentication during transaction. Second trial is allowed if one authentication doesn't work. In case of laptop usage, we use EMV 3DS and local identification. W3C is used for fast browsers.

SECURITY-SCAPE FROM A GLOBAL ANALYST

Brian Reed, Senior Director Analyst, Gartner, was in Mumbai to attend the Gartner Security and Risk Management Summit. He talks about various aspects of security spectrum

Dr Archana Verma
archanav@cybermedia.co.in

Tell us something about your work in Gartner

I cover a number of security related topics at Gartner. I cover security strategy and also security-response. My presentation at the Mumbai Security Conference has been related to Security and response, specifically about insider threats and events related to them.

My work expands globally. I have actually been attending some regional security summits across the world – I am in Mumbai this week, last week I was at Sygney Security Summit, a few weeks ago I was at Brazil Security Summit and I'll be in London in about 2 weeks.

Do you see any difference in the security profile across different regions of the world?

Yes, absolutely, there are some regions that are heavy in things like clouded option. However, in India, we really haven't seen much clouded option, though it is growing; and it will increase in the next couple of years. There is a number of reasons why cloud has lagged behind in India. One of the reasons is that in India many businesses have invested heavily in the on-premise data centres in the last couple of years. Obviously, it takes a long time to work around those capital expenditures invested in a data centre. Cloud security helps in the sense that it's not a heavy upfront cost involved in building a data centre and building a security centre of your own. It saves the money that you spend on operation over the years. If you look at some of the things that we publish, we look at areas like cloud and I think it is really far behind other security markets.



BRIAN REED
Senior Director Analyst
Gartner

Can you elaborate on security management of businesses facing service description?

There's the need to look away from organisations that have several hundred security controls in to basically having a few service descriptions. We also talked

about how to create value in state. Security operations can basically prove value to the businesses. There needs to be some sort of operational gains to be made and some sort of business advantage for security.

What kind of response for a security threat scenario would you recommend?

Yes, in the summit presentation I talked about the security scenario response. Basically, the businesses are very focused on what is very obvious around security. The three incidents that I talked about adding accounting for what compromised credentials, accounting for insiders' threats and also looking at ransomware. It is different from the runoff the mill malware and requires a different solution from a malware.

Can you elaborate a little more on the insider threat?

There is a variety of insider threat personas out there. It's not just eternal hackers, or employees trying to steal your money. There is a number of human psychology elements that you need to take into account while building an insider threat management programme. For example, employees who may be thinking about leaving an organisation, what attributes some employees have; for example, how often they are not logging into the office network system, whether they have frequent absences or unexplained disappearances. Maybe they have a negative attitude. The elements of IT security controls that you might have, impacts the security profile. But there is also the element of human psychology like someone in the office with a negative attitude or someone posting on social media that they're unhappy with their job.

With more and more businesses migrating to cloud across the world, what kind of security threat are going to arise and what solutions can there be for it?

I have been studying top ten projects in 2019, out of which two are directly related to cloud. As the world is moving towards more and more clouded option, there are going to be many different types of security solutions technology and different sorts of tools which will be different from the traditional on-premises security tools. For example, in that top ten security projects, we go into the reasons for some vendors who might give a cloud security product. Cloud access users who use Office 365 may have a repercussion. It's necessary to understand how you're

Cloud security helps in the sense that it's not a heavy upfront cost involved in building a data centre and building a security centre of your own. It saves the money that you spend on operation over the years. If you look at some of the things that we publish, we look at areas like cloud and I think it is really far behind other security markets

Office 365 and if it's in compliance with the security standards.

With the constant evolution of technology, there is a constant evolution of security threats assuming new forms, requiring new solutions. This requires constant investments in security solutions. How do you think this can be managed by the businesses?

Yes, we have seen that. How technology evolves and how it's being delivered. But access to cloud and access to cloud security is a different delivery model. The data centres are very expensive, but cloud technology is really low-cost. Once you go through that initial step of migrating to cloud, there is really not much capital expenditure and you don't need to buy any data centres.

It is being said that IoT devices, as they increase in number, are going to bring more security threats in both software and hardware. What are your thoughts about this issue?

IoT is definitely a security concern, for the reason that you mentioned. If you think about consumer IoT and business IoT, how often they are going to switch off may not be easy to decide. For example, an IoT-connected refrigerator, with food in it. The other point is the software. Many times, the IoT may be manufacturers themselves don't really consider security element. They may have the top credentials, but in many cases their credentials may be a security risk. Sometimes there are default credentials that are not allowed to be changed, which is a big risk.

SECURITY PERILS IN RETAIL SECTOR

Globally, the retail industry is one of the most targeted sectors by cybercriminals and is also at a higher risk. Shailendra Singh, Chief Information Security Officer, Capillary Technologies, speaks on the concerns in detail and what kind of security postures the industry needs to take to protect the business interest as well as to protect the consumers' personally identifiable information

Soma Tah
somat@cybermedia.co.in

Why are retailers most at the risk of data breaches?

The retail industry has a massive customer base and that's the primary reason for being targeted by malicious attackers with the intent to steal data and information. For example, to remain competitive and provide their services in a more customer-centric manner, the retail industry uses many applications such as CRM, Business Analytics and AI & ML solutions etc. which involves handling a massive amount of data to draw useful insights. The retailers are cognizant of the need for security of those data; but hiring expertise in-house will have limited benefits as the software used are not built in-house.

How do you view the security postures of Indian Retailers' in this context?

Indian customers are quite tech-savvy and have adopted newer technologies at a pace that is often faster than the global average. Unfortunately, the same cannot be said about the security awareness of the organizations. This creates an opportunity for malicious elements to target them, whether they are an employee or a customer.

Contrary to the popular belief that the regulatory measures to protect data create a dispute between customers and businesses, they create a more secure ecosystem for both. The problem currently faced by the Indian consumer is a lack of clarity on the benefits. The threat surface becomes larger as the breach can be caused either by those intend to exploit these loopholes or those who choose to ignore the laws for short-term gains.

The primary objective of a customer involved in the act of shopping is to purchase an item that they want and like, while the primary objective of businesses in the retail industry is to be aware of trends, ensure that the retail supply chain functions effectively and the customer gets what they seek. Information security, as



a focus-area, is not the first and foremost thing in the minds of either of these parties and that is not likely to change overnight.

How much of a concern are the non-payment data right now for the retailers?

It is a misunderstanding that non-payment data does not need security. The retail industry collects a lot of personally identifiable information such as names, phone numbers, email addresses, spouses' names, birth dates and wedding anniversaries, which are necessary for their CRM and loyalty programs. This is in addition to the payment data such as card number and payment information. These types of data are valuable information, which is a prized target for malicious attacks. Large databases are frequently targeted and stolen to be eventually sold in the cyber black market, which is also known as the Dark Web.

Further, data privacy laws are changing rapidly across the world. Most of these laws mandate that the data collector undertake adequate measures to protect it. A consent mechanism needs to be built into the system and this is the onus of the InfoSec



SHAILENDRA SINGH
Chief Information Security Officer
Capillary Technologies

Department since Information Security and Data Privacy are closely related.

Brand image is a very important factor in the retail industry. There are a couple of incidents of major setbacks in business performance and the brand images for the retailers following major cyber-attacks. The general customer population does not respond well to news of security breaches. Since the retail industry is B2C, social media buzz about a cyber-security incident commonly results in a wide and deep impact on sales.

What kind of action strategy do the retailers need to take to protect sensitive consumer data?

The activities and rules of information security for the retail industry are not different from those

Privacy-by-design, outsourcing of information security activities and regular reviews of the security posture are the only ways to overcome this problem

applied to other domains. Good information security practices, well-defined and adequately vetted Information Security Management System in the form of Policy, Process and strict adherence to this system are necessary. Obtaining information security certification such as ISO 27001, PCI DSS, SOC 2 along with sufficient effort for evaluating regulatory compliance such as EU GDPR is a useful endeavour.

The cost of maintaining high levels of security has increased a lot in recent times. This cost may be in the form of resources, people, effort, time, or money. But the cost of poor security is usually way higher. In situations where a retailer uses a vendor-provided application, it must be a mandate that they follow secure practices, both technical and non-technical. Regular audits and frequent discussions to ensure that security is a priority for the vendor is highly recommended.

And a retailer should follow the same practices for risk mitigation towards information security as they do for other aspects of the business. Risk mitigation can be done by either taking up activities that reduce risk, or by transferring the risk to another entity, or by obtaining insurance against the impact of a security breach or by changing the practices that effectively eliminate a specific risk.

As retailers embark on a hybrid retail journey, which involves online presence along with the traditional brick-and-mortar stores- do they need to change their overall security postures too?

The primary difference between an offline brick-and-mortar store and an online e-commerce store is the point of data collection. In the first case, data is collected at the PoS while in the second case data is collected at the web application end. Beyond this, almost all aspects of the data flow remain nearly identical. Once the data is collected, they flow to the same cloud environment. Effectively, the only difference in information security strategy that an offline business will apply will be the added security measures that need to be implemented at the store. The moment data crosses the store boundary, it travels in the same manner, as it will when collected through a web application for an online business. This means that almost the same kind of technologies should be implemented in both cases. The primary differentiating factor, which can have the most impact on the security posture of an offline store, will be the security awareness of the store staff. Efforts should be taken to train them on right information security practices.

LAGGING AREAS

Challenges of security in the age of IoT

Dr. Archana Verma
archanav@cybermecurity.co.in

Hardware Security

With the coming of the IoT devices, the concept of security is also undergoing change. While a lot of effort is being used on evolving security software solutions, for many people these security softwares may be expensive and therefore, out of regular reach. In such a scenario, hardware security will be of utmost importance. This gives rise to another problem viz., the skills needed for accessing the security features in x86 in Windows and Advanced RISC Machines (ARM) are very rare. Hence, there is a pertinent need to impart these skills to IT professionals.

Infrastructural security has to do with Networking Functions Virtualisations (NFV), which uses virtual machines (VMs) to manage several functions in the hardware. In the pre-IoT era, the Internet transmits messages without using them for predictive analysis of any kind. But with the coming IoT, messages will be transmitted with many kinds of analytical interpretations associated with them. This will require end to



"In the context of all-pervasive digitisation, rich content delivery, rapid innovation, high speed transactions and every user enterprise turning digital, it becomes imperative for Security to catch up."

**—Rama Vedashree,
CEO, DSCI**

end security. NFV will have to enable it in gateways, transport networks, clouds and DCs. This is a new technology, so the tools and products that enable this security are only coming up at the moment.



"With digitisation comes many possible security threats. Cyber Security comes as part of the system design and today threats have emerged possibly due to gaps in infrastructure or the system, which needs to be addressed. It is

therefore imperative to incorporate it in the system design stage itself."

**—Gaurav Gupta, Principal Secretary,
Department of IT, BT and S&T, Government of
Karnataka**

Cloud and Automation

Clouds will become the only platforms to serve the IoT devices. Cloud technology is compliant with virtualisation of networking, but more designed for data management, processing and storage. Automation and a focus on heterogeneous operating systems will require a security system to serve their unique needs. IoT risk managers have too be trained in this system.

As more and more IT work will be done by softwares, they will have to be imparted with security standards that reduce the vulnerability level. The IoT products are released to the market on a fast track for commercial reasons without developing proper security systems around them. This will need to be addressed by the developers.

As the society moves towards IoT world, it is imperative to address these challenges quickly.

MAJOR SECURITY BREACHES IN 2019

Some flashpoints of Security Breaches in recent months

PCQ Bureau



January



- Personal details of German Chancellor Angela Merkel and hundreds of other politicians of the country hacked and published online
- In his battle with T Series to reach 100 million YouTube subscribers, Pewdiepie gets the support of hackers who take control of 65,000 smart TVs globally as a publicity stunt

February

- Security lapse leaks millions of Aadhaar numbers via the Indane website
- Toyota Australia website and communications go

offline following malware attack

March

- Facebook data breach exposes the passwords of hundreds of millions of accounts

- An internal US Navy review stated that the navy and its industrial partners were under siege by Chinese hackers targeting American national secrets
- America's Jackson County (Georgia) and Albany (New York) hit by ransomware, hundreds of thousands of \$US paid up

April

- JustDial data breach exposes the personal data of 100 million users
- Ransomware hits in America, Augusta (Maine), Greenville (North Carolina) and Imperial County (California)

May

- Israel conducted an airstrike against a Hamas building in Gaza which it accused of conducting a cyberattack. This is the first time that a cyberattack has been met with a comprehensive physical retaliation in real time
- RobbinHood Ransomware in America hits City of Baltimore (Maryland)

June

- NASA announced that its Jet Propulsion Laboratory was hacked the previous year by a Raspberry Pi computer. Through that the hacker reached the NASA network and the Deep Space Network



radio telescopes

- US cyberattack disables Iranian rocket and missile launcher computer systems in retaliation for the downing of a US drone. Russia also claims that US has planted malware on its electric grid systems
- The contracts to fix cyber vulnerabilities in US Air Force's F-15 fighter and C-130 transport fleets bagged by Raytheon
- American real estate title insurance company First American sees a leak of transaction record of 900 million customers, the second largest data breach in history since 3 billion Yahoo! accounts were hit in 2013
- America's Riviera Beach (Florida) pays US\$600,000 ransom in Bitcoin to ransomware hackers

July

- Hackers steal 5 million tax revenue records in Bulgaria—that is of every tax paying citizen in a country with a population of 7 million
- Russian intelligence agency contractor loses 7.5TB of data, FSB's highest till date.
- Unauthorised access gained personal information 100 million plus Capital One credit card customers and applicants to their products
- Equifax agreed to pay hundreds of millions of US\$ as part of its settlement with US authorities over the data breach of 2017, where the personal information of 143 million was compromised

August

- A UN report claims that rogue state North Korea generated US\$2 billion plus over a period of time via sophisticated financial institutions and cryptocurrency exchange cyberattacks
- National Payments Corporation Of India bars Truecaller after its bug created thousands of Unified Payment Interface accounts without the users' consent
- The personal data of millions of customers exposed in online marketplace StockX data breach



Coming soon...

India's tri-service command Defence Cyber Agency (DCA) to counter cyber threats set to be established in November

SECURITY THREATS IN NUMBERS...

As cyber threats increase worldwide, India continues to be vulnerable on multiple fronts and Indian IT teams struggle to keep up with newer and more novel ways of attacks

PCQ Bureau

India's global rank

Network attacks: 1st
Spam: 2nd
Ransomware attacks: 2nd
Source of overall malicious activity: 3rd
Threat from cryptominers: 4th

Source: Symantec ISTR Internet Security Threat Report]

The Cloud situation

- Poorly secured cloud databases continue to be the Achilles heel for organisations
- Over 70 million records leaked from S3 buckets in 2018, typically as a result of poor configuration
- Numerous online tools allow potential attackers to identify misconfigured cloud resources
- Discovery of vulnerabilities in hardware chips also place cloud services at risk: Meltdown, Spectre, Foreshadow

Source: Symantec ISTR Internet Security Threat Report]

The IT team struggle

- IT teams spend 32 percent of their time managing security, yet still struggle with a lack of expertise, budget and up to date technology
- 81 percent Indian IT managers said their organization's cybersecurity budget (including people/technology) is below what it needs to be
- 89 percent Indian IT managers believe staying up to date with cybersecurity technology is a challenge

Source: Sophos Global Survey

Top countries affected by targeted attack groups (2016-2018)

Spear-phishing emails most widely used infection vector, employed by 65% of groups
USA global rank No. 1 with 255 attacks
India global rank No. 1 with 128 attacks

Source: Symantec ISTR Internet Security Threat Report]

Getting more sophisticated

- Threat actors are becoming more organized and business-like by implementing subscription and as-a-service-based business models to deliver malware in an effort to reduce their work and improve their return-on-investments
- Spam is heavily used by threat actors as a conduit to distribute malware. Professional Education was the most targeted sector for spam, as they are likely seen as a prime target due to constantly changing student populations that are not likely to have high security awareness and the potential for attackers to get access to personal data
- Attacks on Management & Consulting and Biotechnology industries accounted for 30% of all impersonation attacks
- Trojans made up 71% of opportunistic attacks

Source: Symantec ISTR Internet Security Threat Report]

Phishing woes

- 1 in 7 businesses experienced lateral phishing attacks in a seven-month period, based on a random sample of enterprise organizations
- More than 60 percent of organizations that were attacked experienced multiple incidents
- About 11 percent of attacks managed to successfully compromise additional employee accounts
- 42 percent of the lateral phishing incidents weren't reported to the organization's IT or security team
- More than 55 percent of the lateral phishing attacks targeted recipients with some personal or work relationship to the hijacked email account
- 37 percent of lateral phishing attacks used tailored content that was enterprise-oriented or highly specific to the victim's organisation

Source: Barracuda Networks Spear Phishing: Top Threats and Trends

Remote Desktop Protocol (RDP) exposes PCs in just 84 seconds

Research based on 10 geographically dispersed, low-interaction honeypots showed that -

- 'administrator' was the most used username by cybercriminals followed by 'admin' and 'user' for login attempts in Mumbai
- 266,448 login attempts made on Mumbai RDP honeypot over a 30-day period
- All 10 of the honeypots received their first RDP login attempt within one day
- Time to first login attempt to Mumbai honeypot was 5:50:06 hours
- The 10 RDP honeypots logged a combined 4,298,513 failed login attempts over a 30-day period. This is approximately one attempt every six seconds

Source: Sophos study

Evolving cybercriminals

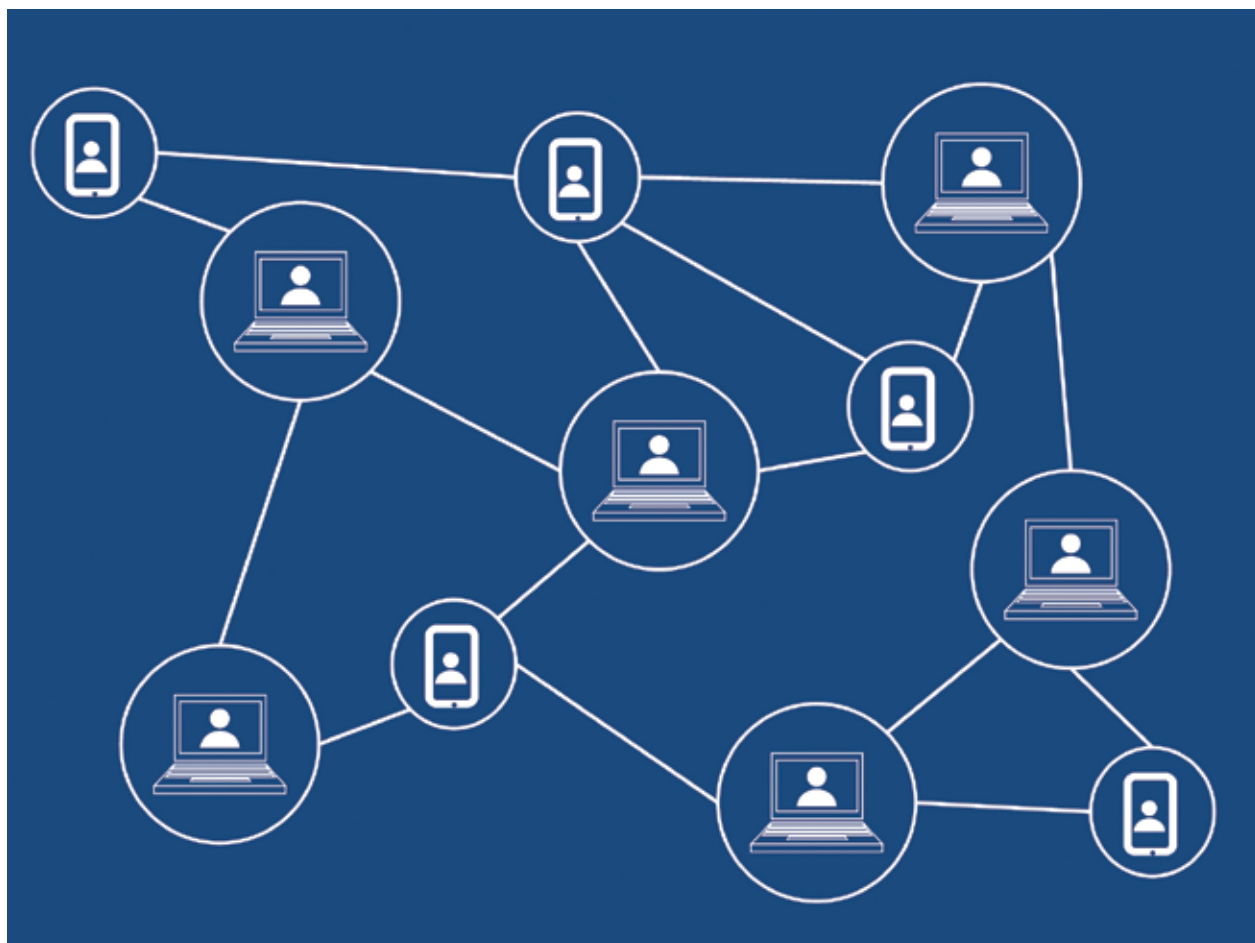
- Cybercriminal tactics have evolved into using multiple attack methods and often multiple payloads to maximise profits
- Software exploits were the initial cause of 41% of incidents and used in 35 percent of cyberattacks, demonstrating how exploits are used at multiple stages of the attack chain
- Phishing emails impacted 54% of those hit by a cyberattack
- Ransomware impacted 39% of attack victims
- 48% of attack victims suffered a data breach

Source: Sophos survey of 3,100 IT decision makers from mid-sized businesses in India

WHY BLOCKCHAIN MATTERS IN CYBERSECURITY AND IN OPEN INTERNET

Blockchain can be used for protecting personal data. It provides identity protection solutions that can be more effective than the existing password-based security as well as multi-factor authentication

Sonit Jain



Blockchain has been among the most talked-about technologies by not only the mainstream public but also business leaders in recent years. However, very few practical applications of blockchain have materialised except in the domain of cryptocurrency like Bitcoin. Blockchain is yet to be tested and used in a context outside of cryptocurrency. However, the technology holds great promise in many fields, from healthcare to law and beyond.

Theoretically, the innate characteristics of blockchain—immutability, decentralisation, traceability and transparency; can be leveraged through numerous real-world applications. Blockchain and smart contracts, which is enabled by blockchain networks, can improve many existing business applications to make them more streamlined, efficient, and secure. And this possibility has been vehemently propagated by the online tech community in recent years, creating the impression that it can solve every conceivable technological problem. Such unrealistic expectations have been among the leading reasons why 98% of blockchain projects have been reported as failures. These inflated expectations also exist when it comes to blockchain's cybersecurity applications.

Blockchain's Role in Cybersecurity

Blockchain is viewed by many as an omnipotent cybersecurity solution and as a means to secure critical data. While it may not be as versatile as people think, blockchain does serve as a secure repository of critical data that cannot be compromised using conventional means. Blockchain uses what is known as a cryptographic hash function which generates a unique string of characters and numbers corresponding to your critical data. And this hashed data can only be decoded with the original cryptographic key that is private and thus hard to replicate. Using a cryptographic hash function, the data pertaining to transactions taking place on a blockchain network can be secured from unauthorised access.

Blockchain-based identity management is a burgeoning field that is expected to grow at a rate of 84.5% by the year 2023.



Sonit Jain, CEO, Gajshield Infotech

That's because blockchain-based identity protection solutions can be more effective than the existing password-based security as well as multi-factor authentication.

On the one hand, password protection is becoming increasingly ineffective against evolving identity theft attempts leading to the need for more advanced ways to secure identity. On the other hand, multi-factor authentication – while being more secure than basic password protection – adds extra steps to the process of verification, causing inconvenience creating bottlenecks in processes. However, identity theft is a highly expensive problem to deal with identity theft crimes cost US\$ 4 billion in 2018. Thus, the need for improved identity and access management for both individuals and businesses will increase in the coming years. Thus, blockchain can become a mainstay enabler of secure yet convenient identity management systems.

Blockchain can be an invaluable asset in combating identity fraud and securing financial transactions. Decentralised identity is a concept that is being rigorously explored in recent years as means to control identity fraud and ensure that people take

In addition to securing critical bits of information, blockchain can also be used for protecting personal data used for authorising individuals to access different services

total ownership of their personal data. To that end, leading organisations like Microsoft are exploring the use of blockchain-enabled decentralised identity. Decentralised identity can potentially replace all existing means of authorisation that rely on email IDs, phone numbers, and passwords. This will enable users to have a globally unique digital identity they can use for accessing any service through digital platforms without having to go through verification ordeals. Such systems will have security and trust inherently built-in eliminating any opportunity for identity theft.

Blockchain's Role in Keeping the Internet Open and Neutral

The shift towards decentralisation and democratisation driven by the rise of blockchain is also lending impetus to the global push towards creating an open internet. The Internet should ideally be an open community equally accessible to all individuals and organisations, regulated by no single entity. However, an open Internet, while being favourable to continued progress and collaboration to drive technological and economic growth, can also become a medium for conducting unlawful activities without enforcement. And this may cause some unrest among people. There is a threat to net neutrality, due to Internet service providers (ISP) who have the power to restrict or favour access to websites of their choosing, hampering fair competition.

Blockchain can potentially act as a solution to ensure an open, neutral Internet. Since blockchain can essentially record any piece of information in a way that is immutable and visible to all, it can be used to monitor ISPs and their allocation of bandwidth resources. This way, any wanton manipulation of bandwidth can be detected and, eventually, deterred

While blockchain holds the potential to revolutionise privacy, security and the Internet itself, it is important to understand that blockchain is still in the early stages of its development. Although it may be well worth the hype surrounding the technology, blockchain faces a few challenges that make it presently impractical to be used in fields beyond cryptocurrency. For instance, blockchain-based identity management systems can only work feasibly when adopted as a platform used by a large volume of users and nodes. However, the technology currently cannot be scaled to be efficiently operated by a large number of users. Using blockchain in its existing state cannot handle the speed demands of mainstream applications.

For instance, the Bitcoin blockchain can handle only 7 transactions per second, which is much slower than the current centralised transaction and security systems.

It is right to be enthusiastic about a blockchain-driven future, which may allow us to enjoy unprecedented benefits, in terms of security, convenience, as well as financial gains. However, as businesses, it is important to be cautious while considering blockchain-based applications for critical functions like cybersecurity for at least a year or two now.

The author is CEO, Gajshield Infotech



MAKING INDIA “MAN-IN-THE-MIDDLE” ATTACK FREE

MITM (Man-in-the-Middle) attacks, or more popularly known as session hijacking are becoming the norm as we move into the era of emerging tech. Some thoughts about this

Dr. Ajay Data



Data Breaches

India's Internet users are expected to register robust growth, nearly 18% annually and expected to reach 650 million by 2020. As India makes

deep Internet penetration, safeguarding digital infrastructure against cyberattacks becomes paramount. Data and email security are major areas of concern in the times of the digital revolution.

The companies are undergoing a phase of digital transformation and MITM attacks in terms of theft of digital identity and online brand impersonation have become very common. Moreover, the loss of intellectual property and malware infection also surfaced as the top security blind spots. They have high levels of business impact and long recovery times and in many cases neither Government nor companies can afford it, the Frost & Sullivan study said in its report.

Securing Data

Not using emails is not the way out. What is important is to ensure that the emails sent to colleagues, customers, vendors, etc are as secure as possible. One should always be sure of what information he/she is sharing and with whom. One should take care of not including any suspicious email ID to our mailing list to ensure that the information does not get into the wrong hands. Sending information of utmost confidentiality through emails should be avoided. It is always better to ensure that it is thoroughly encrypted. Even while receiving emails, the country must take special measures to let citizens be protected from phishing attacks and protect them from these “get rich” scam emails and identify theft emails.

It has been found that almost 2-4% of emails contain virus which means that an unimaginable number of emails with viruses are circulated every day. We need to execute a multi filtering arrangement that will check email connections with various antivirus engines. By utilizing the intensity of the distinctive algorithms of each engine, identification rates have expanded, giving robust security against such malware.

In addition to sophisticated hardware, it is important to take care of measures to avoid falling prey to hacking, cyber security issues or data leaks. Certain practices are small and easy to implement but help negate the problem to a great extent



“It is unimaginable to calculate the amount of data shared over email. Moreover, it is equally risky, especially when unethical hacking and cyber breach become regular practices. Simple solutions like antispam and antivirus software are no longer enough. The security teams need

to understand the ever-evolving protocols and remain ahead in the learning curve for possible attacks.”

—Dr. Ajay Data, CEO, Data Xgen Technologies & Chairman, Universal Acceptance Steering Group (UASG), ICANN

Digital Defence along with email security will remain an issue. Some very innovative and secure solutions have been designed to address such issues. One of them is enterprise email platform XgenPlus, designed and developed in India by Data Xgen Technologies. It has features that can take care of the above-stated security issues and also offered many secured frameworks to keep the hackers at bay.

Three Critical Areas

There are three critical areas we need to focus on. MITM can be tackled with PKI technologies if the governments mandates S/MIME for emails, SSL (Secure Socket Layer) for all kinds of websites, cloud hosting, and API (Application Program Interface) access for mobile apps and IoT devices. Such a mandate can help making our systems MITM Attack free. This will be a good target to achieve and declare India free from MITM Attacks. Digital Infrastructure needs to be enabled to break the language barrier to bring next billion people online. In a nutshell, we need to ensure that while pushing for Digital India, we need to also stay ahead in the security curve with Secured India.

The author is CEO, Data Xgen Technologies & Chairman, Universal Acceptance Steering Group (UASG), ICANN

NETWORK SECURITY & CYBER RISK MANAGEMENT IN INDIA 2019-2024

Focus on Aerospace & Defense, Retail, Government, Healthcare, IT & Telecom, and BFSI Verticals

PCQ Bureau

The network security and cyber risk management market in India is expected to register a CAGR of 11% during the forecast period, 2019-2024. In the past, India has been targeted through cyber-attacks primarily for political reasons and trends show that this landscape seems to only gain prominence with the availability of more sophisticated technology and more complex transactions increasing the vulnerability of systems.

Key Highlights

- Government initiatives aimed towards digitizing Indian industries is expected to be the major driving factor for the market. Government schemes such as Make in India, Start-Up India and Digital India supplements the growth of Cyber Security market in India and is a linking pin towards Public-Private Partnership (PPP) models.
- In India, Critical infrastructure is owned by both Public Sector and Private sector, both operating with their own norms and protocols for protecting their infrastructure from cyber-attacks. But there is no national security architecture that unifies the efforts taking place in the public sphere and in the private sphere.

Major Market Trends

Intrusion Detection & Prevention System to Dominate the Market

- An Intrusion Detection and Prevention Software (IDPS) monitors network traffic for signs of a possible attack. When it detects potentially dangerous activity, it takes action to stop the attack. Often this takes the form of dropping malicious packets, blocking network traffic or resetting connections. The IDPS also usually sends an alert to security administrators about the potential malicious activity.
- The two main contributors to the successful deployment and operation of an IDS or IPS are the deployed signatures and the network traffic that flows through it.
- According to Insider Threat 2018 report, most insider exploits are detected through IDPS. This indicates the popularity of IDPS and why majority of the vendors are offering this service.

Growth in Mobile Phones to Significantly Drive Market Growth

- India has seen a tremendous growth in tech savvy

population, with mobile phones being the first digital medium.

- Since its launch in August 2016, Jio added 200+ million users, representing 18% of the mobile subscribers market in India. Jio helped establish 4G in India making it affordable for people of all financial backgrounds.
- As 2G users decrease with every passing month, 3G and 4G will lead the mobile internet path till 5G is launched.
- At the same time, there has been substantial growth in IT spending in India and scaling up in the use of technologies such as Internet of Things (IoT), Cloud Computing, Artificial Intelligence (AI) and Block Chain.

Competitive Landscape

The market is fragmented due to rise in users who consume data in vernacular languages, growth in travel transactions or e-commerce transactions and new users from rural areas. This is causing internet users to grow thus growing need for cyber risk management.

Notable Developments

- May 2019 - Instasafe partnered with ES&S to provide its powerful SDP Security for ease of hybrid cloud adoption. InstaSafe provides a secure platform to adopt cloud computing that increases the productivity of organizations with its ability to connect remote users, vendors & contractors to work securely from any device or location.
- October 2018 - Indian cybersecurity firm Lucideus said that it has raised USD 5 million (over Rs 36 crore) in funding, led by Cisco Chairman Emeritus John Chambers. The funds were used to expand the company's further reach in India.
- June 2018 - Telangana Government partnered with Data Security Council of India to set up a Cybersecurity - Center of Excellence in order to accelerate the state's cybersecurity momentum and position it as one of the leading Indian cybersecurity hubs in next 5 years.

Source: Research and Markets/

<https://www.globenewswire.com/news-release/2019/07/15/1882464/0/en/Network-Security-Cyber-Risk-Management-in-India-2019-2024-Focus-on-Aerospace-Defense-Retail-Government-Healthcare-IT-Telecom-and-BFSI-Verticals.html>

GLOBAL DNS THREAT IN 2019

Understanding the Critical Role of DNS in Network Security Strategy

Romain Fouchereau and Konstantin Rychkov



Executive Summary

Many high-profile breaches and publicized security issues in enterprises have been widely exposed in recent years, demonstrating that traditional security products are no longer adequate and will not provide business continuity or data protection in a rapidly changing environment. The IT security threat landscape is continually evolving. Digital transformation is being driven by the fast adoption of cloud services, and there are major changes linked to the regulatory upheaval we have seen with the enforcement of GDPR, among other privacy initiatives. DNS is a primary target for cyberattacks, causing business damage in terms of downtime and financial loss, as it remains one of the critical elements in delivering IT services.



82%
Companies that experienced a DNS attack



9.45
Average number
of attacks per
company



\$1.07M
Average
damage cost



63%
Companies that
suffered application
downtime

DNS is more than ever a central network foundation, enabling all clients to access every app. Any DNS performance impact has major business implications.

At the same time, the fact that most traffic first goes through a DNS resolution gives it unique visibility over legitimate and malicious network activity. This is being widely recognized by businesses, who are starting to leverage DNS for their security strategy via threat intelligence, policy control and automation.

DNS is fast becoming the guardian of networks!

David Williamson,
CEO, E翻 cientIP

"

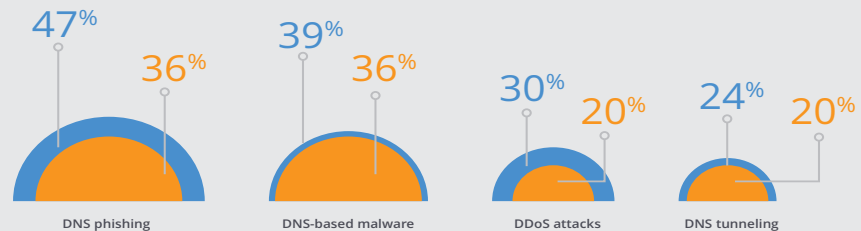
DNS Threat Landscape is Dangerously Diverse

The number of companies that suffered DNS-based attacks has again increased, growing 5% over 2018, and reaching an alarming 82%.

By nature, DNS is an open service to the network, and its mission-critical role for routing application access makes it a primary attack vector and target for hackers. The spectrum of DNS attacks illustrates this fact; compared to last year, it is much broader as the percentage of each attack type suffered has significantly increased, from volumetric to low signal attacks.

Top DNS-based attacks suffered

● 2019 ● 2018



Average number of DNS attacks

2019: 9.45 up from 7.08 attacks in 2018

Source: IDC DNS Survey 2019 n=900

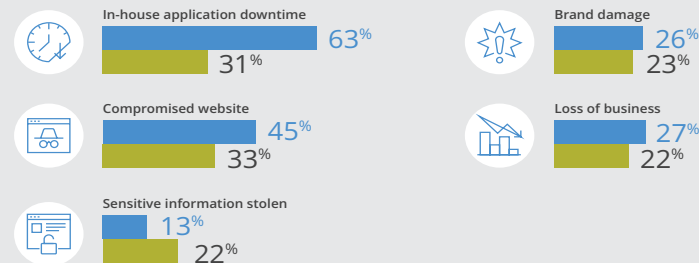
Impacts and Costs of DNS Attacks

2018 saw a strong increase in how organizations were impacted by DNS attacks. Worryingly, both in-house and cloud applications were damaged, with growth of over 100% for in-house application downtime, making it now the most prevalent damage suffered.

DNS attacks are moving away from pure brute-force to more sophisticated attacks acting from the internal network. This will force organizations to use intelligent mitigation tools to cope with insider threats.

Impact Statistics

● 2019 ● 2018



Average cost per attack continues to increase (+49%):

2019: \$1.07M
2018: \$715k

Source: IDC DNS Survey 2019 n=900

State of DNS Defenses

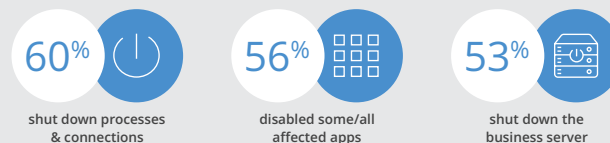
Given the level of damage suffered, awareness of the critical importance of DNS security must improve:



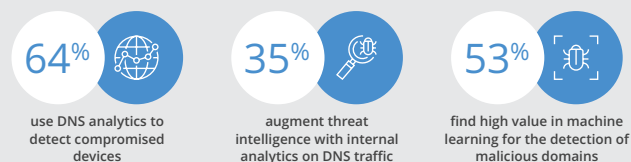
Only **64%** of companies estimate DNS security is critical for business

Conventional security solutions such as secure web gateway, next-generation firewall, data loss prevention (DLP), and intrusion prevention systems (IPS) are not designed to ensure DNS service availability and integrity.

Security countermeasures are based on workaround



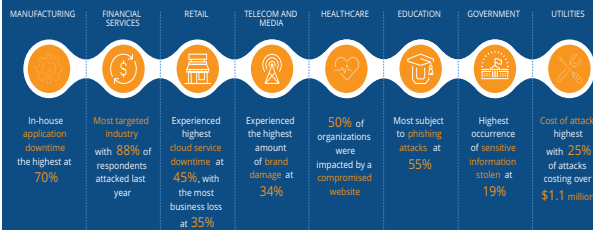
DNS analytics usage is evolving from threat remediation to predictive security



DNS security practices must move from reactive to proactive



No Industry is Spared From DNS Attack Disruption



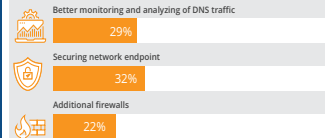
Data Privacy & Compliance, One Year After GDPR

24% of organizations were victims of DNS tunneling last year

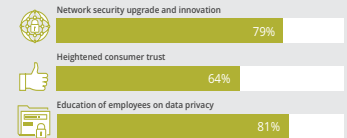
GDPR regulation has been in force since May 2018. Important investments have been made by organizations in all countries, notably to strengthen network security defenses. As part of a security technology strategy, DNS traffic monitoring analysis is considered one of the most effective ways to protect data confidentiality.

Organizations see a positive impact from GDPR legislation, feeling it will sustain the need to deploy stronger security defenses. Ongoing data privacy compliance initiatives strategies in other countries (CLOUD Act, NISD, PDPA, etc.) will also benefit.

Action considered most effective to protect data confidentiality



GDPR Impacts



Network & Information Systems Directive

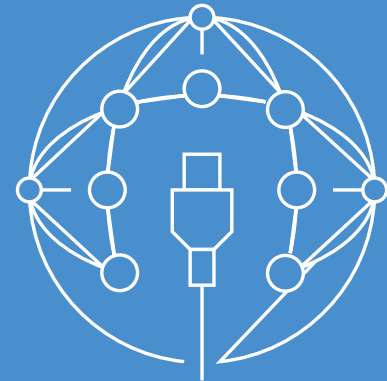
As one initiative to increase Europe's preparedness to ward off cyber incidents and to achieve consistent protection against cyberattacks across all member states, the EU adopted the Network and Information Security (NIS) Directive in August 2016.

The NIS Directive is focused on the protection of essential services and digital services such as online marketplaces, online search engines, and cloud computing services.

The initiative has a broad focus on protecting infrastructure, including physical assets, and there is a primary emphasis on resilience, incident management, and business continuity management.

DNS is critical to ensure service continuity. Faulty or ineffective DNS services can negatively affect the perception of any organization (from clients, partners or employees), impact your ecommerce applications, resulting in lost revenue, and ruin a brand image: 63% of organizations suffered app downtime as a direct result of a DNS attack last year.

When under DNS attack, utilizing adaptive countermeasures designed to ensure DNS service availability and integrity are required: disaster recovery and avoiding single points of failure must be part of the mitigation process and security best practices, as current countermeasures such as disabling all apps or shutting down servers will no longer be suitable.



Zero Trust is Taking Off

Digital transformation leads to a dramatic increase in network complexity and security risks, driven by the proliferation of devices, hybrid cloud, and multicloud deployments, and mobility.

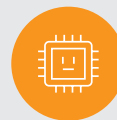
To face these challenges, perimeter network security is evolving to become zero-trust strategy. The new architecture pattern relies on the fact that there are no longer trusted and untrusted zones, perimeters, devices, and users. Everything is untrusted — by default.

A zero-trust strategy requires moving from macro-segments to micro-segments that could be as small as a single client, resource, or server. It implies collecting telemetry data to get in-depth visibility on end-point behavior to detect threats at the most granular level. It also needs advanced automation through a software defined network (SDN) in order to provision micro-segments to connect end points and activate associated filtering security policies.

DNS security, fueled by threat intelligence and network automation, is key to a successful zero-trust strategy.



17% of companies run on zero-trust architecture already, with 48% planning as part of security strategy.



Only an average of 14% collect DNS logs and correlate them through machine learning.



Predictive analytics are already part of the security stack for 45% of companies

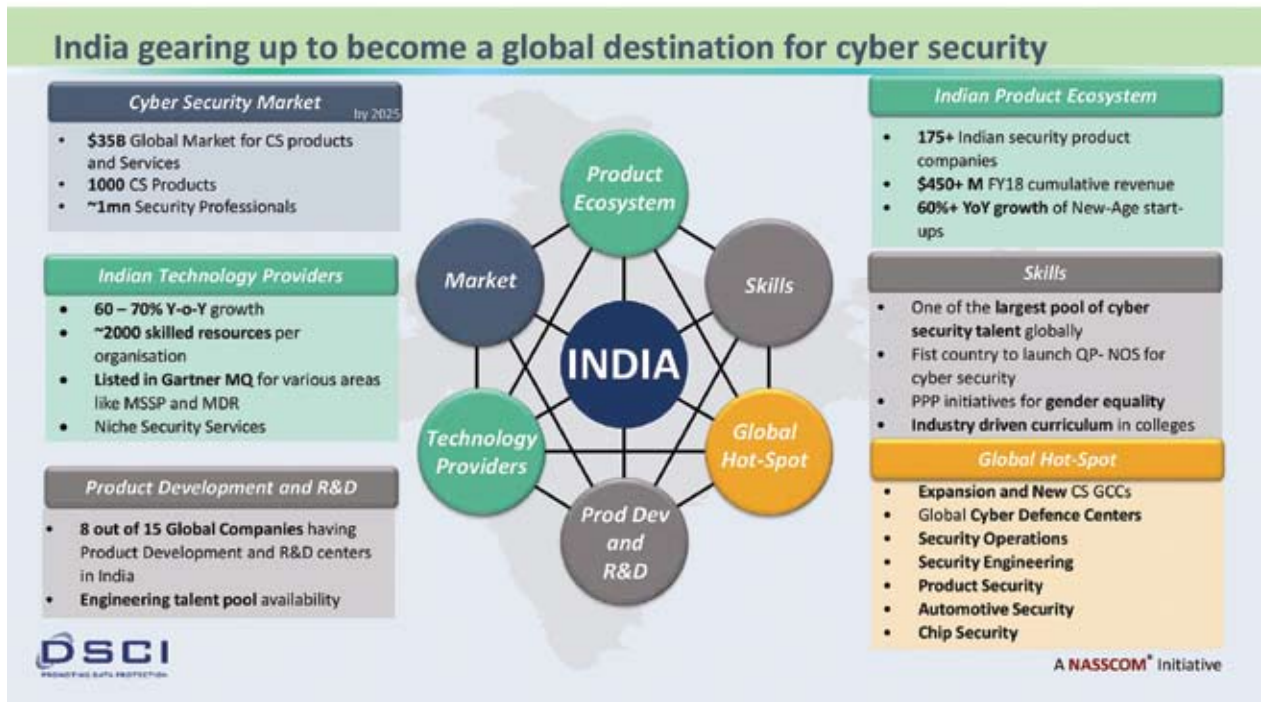


Only 14% have adopted automation in their network security policy management

Romain Fouchereau is Research Manager, IDC; Konstantin Rychkov is Research Manager, IDC CEMA
Source: IDC

INDIA IN THE SECURITY HUB

India is making an effort to tackle its security problems across sectors and is attempting new innovations



AI CAN PAVE THE WAY FOR MORE IMPACTFUL DIGITAL BUSINESS MODELS

Whether it is demand planning, future sales forecasting, turnover predictions, pricing, or market optimisation, analytics is simplifying our lives while reaching the ultimate aim of digital transformation

Jim Brady



Today, digital transformation has taken an all-new meaning for enterprises globally. It all comes down to improved customer experience, enhanced operational effectiveness, and developing newer business models. Artificial Intelligence and analytics are changing the world at an incredible pace.

IoT and Industry 4.0...

AI and IoT are just a few levers of the trend that have kickstarted what some people call the Industrial Revolution 4.0. Enterprises globally are using AI in line with their business goals whether it's to continually revamp their operational effectiveness or innovate on customer experience. With the right attitude and approach, AI can pave the way for newer and more impactful digital business models as well.

We're all heading towards a smarter and more intelligent future and the critical thing to do when you are on the trajectory of change is to embrace it! We must get on to the curve of learning and work on strengthening the base to an AI-intensive future.

Optimism about AI...

I'm an optimist and I believe that the evolution of AI may reduce some jobs but in the long run, lead us to different careers. The retraining and retooling of the workforce will become paramount to organisations in the age of AI. Retraining the workforce rests on the working of individuals, the private sector, and the government.

Big Data, AI and the Changed Role of CIOs and Leaders...

The intervention of Big Data and analytics enables

While the onus will be on the individual initiative to keep upskilling oneself, even enterprises and the government will need to intervene and strategise on how to enable an AI-inclusive world



“Decision-making has evolved from being an anecdotal call taken by leaders to a scientific, algorithm-led approach. Enterprise wide-digital transformation is a reality across the globe. We are poised at the edge of a promising future.”

**—Jim Brady, Advisor,
BRIDGEi2i Analytics Solutions**

CIOs and leaders to make data-powered decisions. Algorithmic accuracy and innovation have changed all facets of a business – whether it is demand planning, future sales forecasting, turnover predictions, pricing, or market optimisation, analytics is simplifying our lives while reaching the ultimate aim of digital transformation. What BRIDGEi2i is doing is democratising information so that data-driven insights are available throughout the enterprise, so each employee can take the next best decisions.

The author is Advisor, BRIDGEi2i Analytics Solutions

IS ARTIFICIAL INTELLIGENCE SHAPING THE FUTURE OF ERP SOFTWARE

The AI-enabled ERP systems automate routine responsibilities and make them as effortless as possible; freeing up your employees' valuable time to focus on tasks that would add to the profitability of your business

Ali Hyder



In the foreseeable future, Artificial Intelligence or AI would have a profound impact on almost every piece of software available in the market, including Enterprise Resource Planning (ERP) systems, in some form or fashion. AI in ERP is going to affect the very essence of the system-controlled business operations.

While AI technology is still in relative infancy, the new Machine Learning is making serious waves in the software market and making inroads into business management applications, endowing them with the power of superior governance structure.

Impact of AI on Industries

AI has the potential to bring change on a wide

scale to companies, where the customer and operational data is primary to the business. Naturally, it's unfair to single out any one industry vertical. Every industry has its share in the benefits, the impact of the new technology is most prominent in process-heavy and data-intensive sectors that have the highest dependency on future predictions done on the basis of historic information.

AI can help the companies organise a large volume of data and turn a limitation into an opportunity. It has tremendous opportunities to augment human capabilities across industries. The technology is transforming systems through creativity and agility.

AI in manufacturing

Manufacturing industry is already using augmented reality and predictive analysis tools. With the introduction of AI and machine learning, these companies can take a leap into a digital future to achieve most improved process optimisation.

AI technology augments manufacturing efficiency to ensure faster production is less time. Right from planned preventative maintenance to every other operation performed in any manufacturing plant, AI would revolutionise them and make them more efficient and less prone to errors.

AI in retail

AI would bring change in the way retail businesses functions today. It would enable retailers to use augmented and virtual reality functionalities in advertising. Introduce immersive product catalog visualisation to dramatically improve shoppers' experience with the products even before they buy.

In the near future, chatbots in retails would have improved conversation capabilities. They would be able to capture the emotions and mood of the customers, basis of which provide emotional responses. In short, AI would empower you to offer immaculately personalised responses to your customers' queries and significantly improve customer loyalty.

What AI-enabled ERP system would be like

AI as a part of your ERP system would affect the very essence of daily operations. The smart technology recognises the users' behaviour pattern and automatically performs the routine tasks they do in the blink of an eye while maintaining an unprecedented level of accuracy. In order to experience this advancement, you need to revise the current technology strategies of your business and be prepared to embrace the change and adapt to the developments.

AI is transforming the way ERP functions

Inclusion of AI in ERP systems makes them more powerful business management tools. Here are the three primary benefits of the new technology –

1. Identify the problems even before they occur

AI integration improves forecasting capabilities of an ERP software. It includes advanced algorithms that can search through and analyse the massive data sets collected in the ERP system, identify the trends, and make predictions about the upcoming periods.

“Artificial intelligence is bound to transform the future of ERP solutions. The new machine learning technology that appears to emulate human actions would influence businesses, regardless of size or industry.”

–Ali Hyder, Group CEO, Focus Softnet



This way, an AI-based system is able to pinpoint or detect the possible problems, enabling users to prepare in advance and even prevent them. AI-run ERP systems enable you to unlock the hidden potential of your business data and use it to manage functionalities with optimal efficiency.

2. Automates routine tasks with system intelligence

You need to follow a defined set of methodology while performing any given task within your ERP system. AI tools can function in a similar fashion. For this, an AI system needs to be programmed with a set of governing rules against each action. The technology is intelligent enough to apply these assigned rules to make decisions that are accurate and at the same time much faster compared to any human.

3. Improves user experience through interaction

One of the main functions of AI technology is to provide intelligent outputs based on human inputs. Artificial intelligence system can read historic data and learn from earlier behavioral patterns of the users. This makes AI-enabled ERP applications provide an extensively personalised experience to the user as well as function faster and in a more useful way.

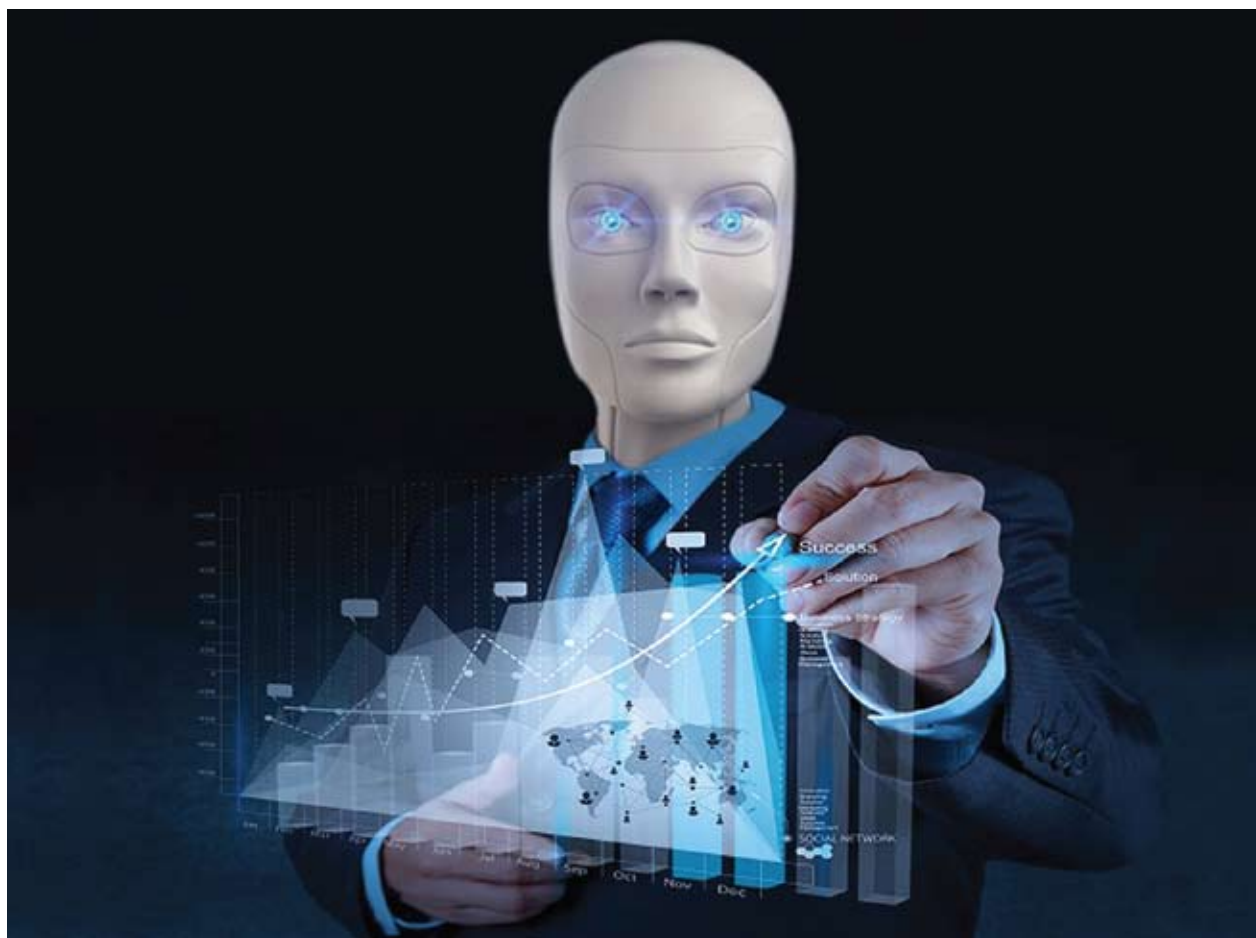
Although AI has not fully arrived, it is going to be a part of the ERP systems in no time! So, you must be ready for this adaptation if you want your business to sustain and remain competitive in the years to come.

The author is Group CEO, Focus Softnet

CONVERSATION GATEWAYS: THE HOLY GRAIL OF CUSTOMER EXPERIENCE MANAGEMENT

Over 2 billion digital, real-time conversations take place every day. People are spending more time on digital platforms than ever before

Nishith Patnaik



It's not uncommon for us to switch on Alexa as soon as we enter our homes these days, and one can't even imagine driving through a new route without the Google voiceover in the background. Conversations have always been important for us, but the key difference today is that it has evolved beyond

simple human conversations. In the current scenario, we have chatbots and voice assistants at our disposal round the clock.

Over 2 billion digital, real-time conversations take place every day. People are spending more time on digital platforms than ever before. A Cognizant report

on Conversational AI states that “85% of businesses believe that immediate online help would improve online sales conversion rates.” However, the question of how businesses can consistently aid their customers remains an unanswered one. In today’s competitive world, customer engagement and retention should be on the charts for every business.

The Era of Conversational AI

Conversational AI has made the concept of omnichannel businesses possible. Instant responses help brands solve customer queries much faster and much more seamlessly, which in turn increases the likelihood of conversion. Chatbots make a great engagement tool. Customer engagement accelerates conversations which in turn drives stickiness. This then drives retention of customers and delivers growth.

Today, every business either has a chatbot, or is considering one. Gartner has also predicted that 40% of mobile interactions will be managed by smart agents by 2020. With this kind of tech intervention, there’s a possibility that consumers will give up on calls and turn to only messaging. This also leads us on to think about better touchpoints for consumers to interact with during the post purchase stage.

The AI in Conversational AI

Artificial Intelligence or AI is the brain behind all these machines which are trained through complex systems like deep learning. To break it down further, deep learning is a simple guide or a flowchart that trains the machine to behave like humans. Innovations like voice assistants, chatbots and IoT devices bridge the gaps in connectivity, and make for better interactions between the brands and its users. Machine learning and deep learning algorithms also ensure that consumer data is tracked, mapped and

Businesses are now able to provide personalised support to consumers throughout their usage journey. Conversational AI has become almost synonymous with increased productivity and greater customer satisfaction across global industries



“Customer convenience management, the modern approach of being there for the user whenever they need support is also catching up. And here lies the most important question: How to

be there for the customer when it matters the most?”

—Nishith Patnaik, Co-founder, Nhance Now

analysed, thus enabling the brand to monitor each individual’s customer behaviour.

Omnichannel Presence

A true omnichannel presence means that a customer always has access to two-way communications with brands. Customers feel obliged when brands pay special attention to them offering relevant services. So, you’re not only focusing on customer satisfaction, but also taking a step towards customer delight. A simple conversation beginning with a greeting can go much beyond, and lead brands to derive significant insights about their past behaviour and purchase history. With this in place, providing recommendations for future needs also becomes simple. The entire customer relationship management process becomes much more streamlined with data.

Integration of AI and Human Intelligence

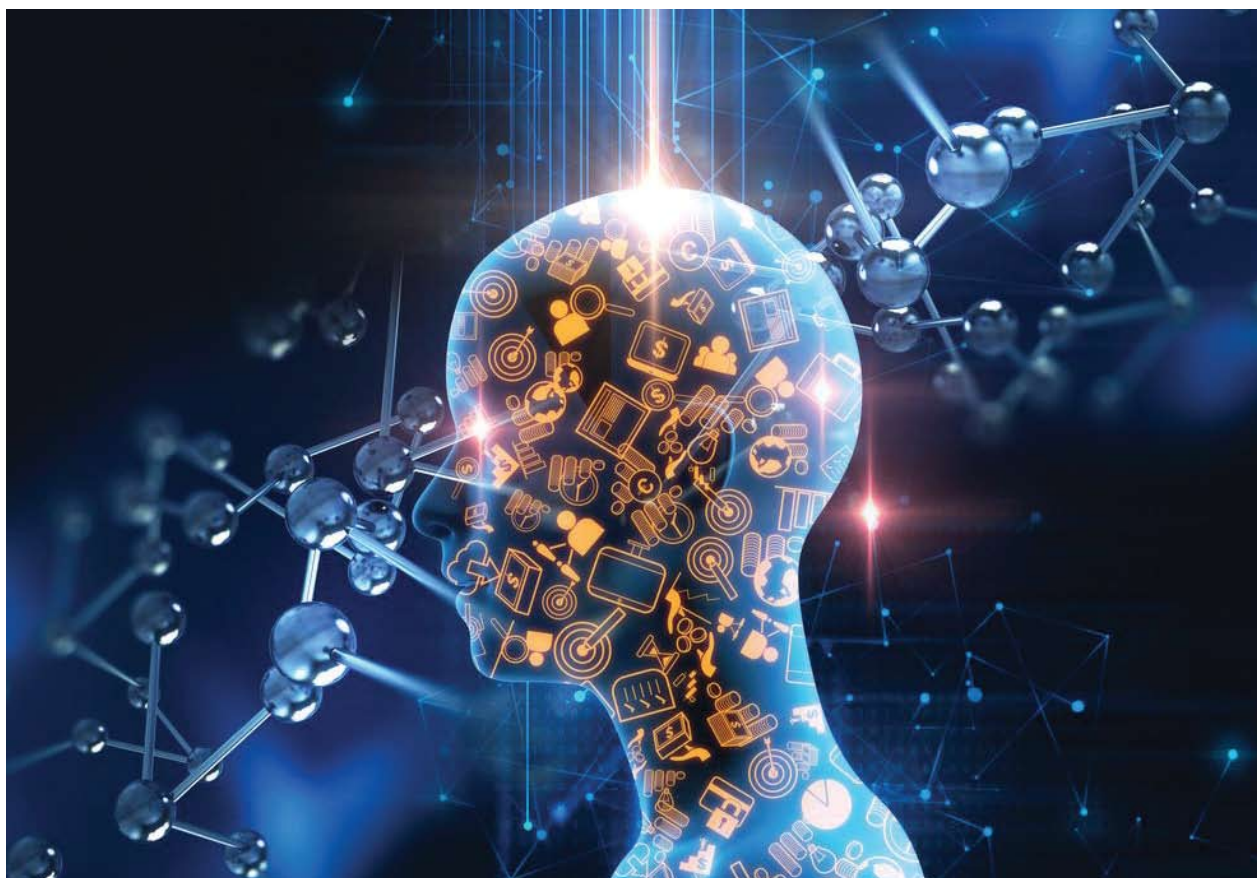
The best of AI technologies has made it possible to understand and predict customer behaviour. Automated speech recognition technologies help the processor understand the customer despite the various background noises. The integration of human intelligence and artificial intelligence is helping technology disrupt and learn the complex human behaviour. Human intelligence being the secondary source is training AI to be a better version of its own self. It just gets smarter with every interaction.

The author is Co-founder, Nhance Now

ADOPTING AI: HOW TO ENSURE SMOOTH IMPLEMENTATION

The C-suite is confronted daily with the speed of technology evolution, under pressure to transform their organisations to stay competitive, relevant and prepared for the next wave of change. AI is one area where management is certainly encouraged to have a strategy. Much has been made of AI's business capabilities in recent years, however for organisations of all sizes, knowing where to start with AI adoption can be bewildering

Charles Ng



Artificial Intelligence is exciting technology, and executives understand that becoming digital is no longer optional. True transformation is a journey however, and for businesses that want to move into the future and be ready for inevitable adaptation and evolution,

it's much more than a case of sticking on a few technology patches. Business transformation takes discipline, vision and fortitude.

For companies starting out in Artificial Intelligence adoption, the most important thing is for management to be on board, because adopting

AI into any part of the business will require change. Without the buy-in from the top, there will be too many hurdles to overcome when it comes to financial investment and inevitable cultural shifts.

How does AI be Effective?

At its core, AI is using data analysis, models and algorithms to make better business decisions. For AI to be effective and for business leaders to see the improved efficiency, productivity and insights they are looking for, it needs access to good data. Management needs to define the metrics it cares about (for example, more accurate customer outreach? More timely purchasing to reduce overstock and waste?) and commit to making decisions from the data as much as possible. Knowing what you want to achieve will make implementation more effective- and you can start with just one process or area of your business. A commitment to data-driven decision making will ensure you're collecting the right data; that engineering systems are in place to handle, manipulate and store data; that you value technical and analytical talent; and that you're shifting the company towards a data-driven and innovative culture.

Company Culture

Company culture has a huge role to play when it comes to bringing Artificial Intelligence into the organisation. People will naturally be hesitant about shifting from making decisions based on experience and human judgment to data-driven decision making. AI has become somewhat sensationalised, making people nervous that they'll lose their jobs to machines. For this to happen soon is unlikely, and instead, AI should be introduced more like a wonderful new team member with the capability to make things more efficient and effective for everyone.

Business leaders might worry that not being fully 'tech literate' is a hindrance to making decisions about AI adoption, but all executives truly need is an appetite for change, an open mind and a willingness to communicate with staff

Proper research is critical to identify the best AI solutions. It's vital for management to have full visibility into what's happening at the organisation every day and to not make any assumptions

The specific resources that each organisation needs to effectively adopt AI technology will depend on what is already in place. Larger organisations might have access to a team of data scientists because these companies will already have platforms in place for them to work from. Data science talent is in high demand and is expensive, which means that small and medium-sized businesses are most likely to bring AI into the company through the help of a vendor.

To ensure the selection of the best solutions, the leadership team must go out into the company and have open conversations about the challenges staff are facing. With this insight, management can work with teams and individuals to evaluate the best products and platforms. Some solutions might require customisation to best perform, so CEOs must be patient while systems are adapted to best serve the organisation.

The capabilities of AI are vast and it can support business operations in many ways. Most organisations want to do things more efficiently, and AI can make tasks scalable. For example, it can take on work that would typically require a team of several people, allowing the organisation to stay lean. It can also relieve people of grunt work- such as repetitive administrative tasks; and give them more time to focus on projects that requires human intelligence and creative problem solving.

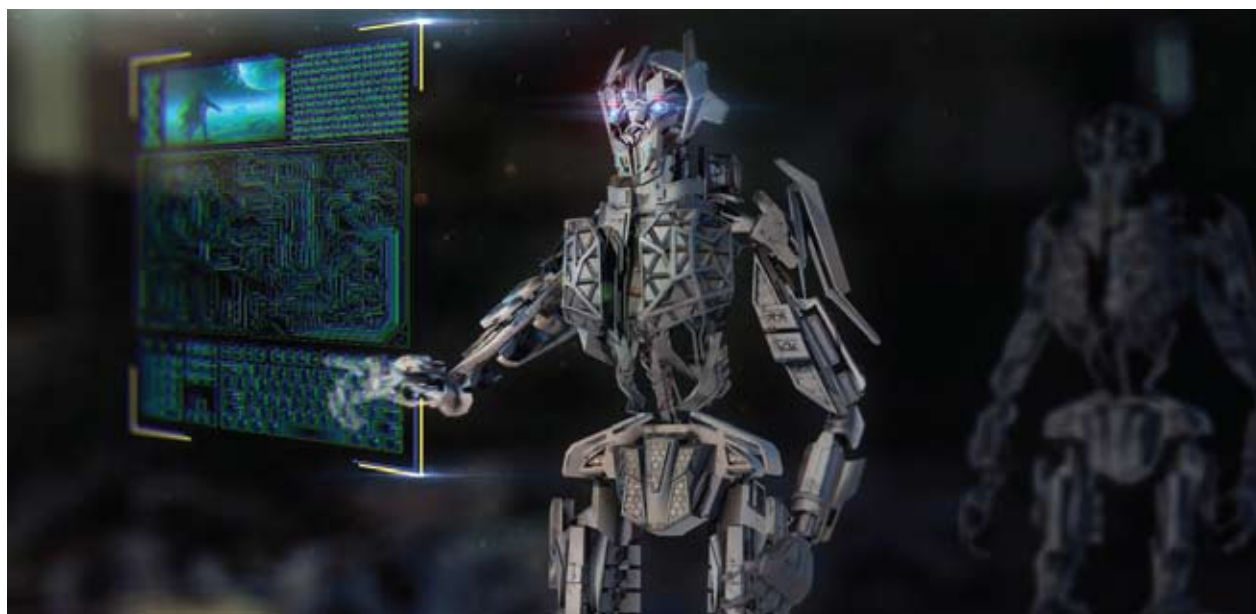
It's an exciting time for AI adoption in India and beyond. The organisations who lead the way will lay the foundation for adoption of new technology that will benefit both business and society. There will be many more advancements in AI, but business leaders cannot wait for the 'latest thing' to make decisions. Rather, they need to work with technology and talent that have the flexibility to adapt and upgrade as AI advances, leading us into a world where products and services are better customised to suit our needs and mundane tasks are automated so we can spend more time on the things important to us as human beings.

The author is VP of Enterprise AI, Applier

AI MAKING BREAKTHROUGHS IN INDIAN BANKING AND HEALTHCARE

India is helping many sectors incrementally, explains Asoke K. Laha, President & CEO, Interra Information Technologies

Sunil Rajguru
sunilr@cybermedia.co.in



Is AI gaining traction in the Indian market in 2019? What are the examples of the businesses that are implementing AI-ML?

Undoubtedly, AI, ML and IoT are gaining ground in India in a relative sense. It is often said India is the third largest country where these cutting edge technologies have been put to use, the first two being US and China. But we are far behind both countries in these segments, being a late comer. The real battle for supremacy is being fought between US and China and the rest are peripheral players. My sense is that countries like South Korea, Finland, Sweden, Russia etc are ahead of India in the R&D and incubation in AI-ML and IoT.

There will be significant progress in these technologies in 2019 and beyond since almost all top Indian companies are drawing up plans for implementing these technologies. The sectors that are attracting digitalisation/automation are retail banking, healthcare, IT, infrastructure, education, healthcare and the list is expanding. Let me point out

a few examples.

A lot of banks have already adopted AI-based systems to provide customer support, detect anomalies and credit card frauds. An example is HDFC Bank. It has developed an AI-based chatbot called EVA (Electronic Virtual Assistant), built by Bengaluru-based Senseforth AI Research. Eva has addressed over 3 million customer queries, interacted with over half a million unique users, and held over a million conversations. Eva can collect knowledge from thousands of sources and provide simple answers in less than 0.4 seconds. It is also used for fraud prevention.

What are the AI trends in both India and worldwide? Where is India lagging when it comes to the rest of the world?

I feel AI and related technologies are incrementally impacting sectors like marketing, banking, finance, agriculture, healthcare, gaming, space exploration, driverless cars and chatbots. Looking at the healthcare

sector, there are many examples of AI use. Cambio Health Care developed a clinical decision support system for stroke prevention that can give the physician a warning when there's a patient at risk of having a heart stroke. Another such example is CoalaLife, which is a company that has a digitised device that can find cardiac diseases. Similarly, Aifloo is developing a system for keeping track of how people are doing in nursing homes, home care etc.

Space expeditions and discoveries always require data mining. AI-ML are the best way to handle and process data on this scale. Astronomers are using AI to sift through years of data obtained by the Kepler telescope in order to identify a distant eight-planet solar system. Tesla will have "robotaxi" version – one that can ferry passengers without anyone behind the wheel – ready for the streets next year.

Yet, the point to be noted is that India is lagging behind in the fundamental research in these technologies. Also, I feel in the Indian situation it should be put to use more widely and intensely in sectors like cleaning of sewerages, rivers, oceans and other water bodies, or for ensuring better security checks at airports and public transport systems.

Will AI see a fillip in 2020 and what about the entire 2020s?

According to Gartner, 2020 will be a year which will be important for the development of business related to AI. This is because computerised reasoning will become a positive spark of work. With the arrival of 2020, job creation related to AI will cross into positive territory, reaching two million new jobs in 2025.

Are there any dangers of AI? Can it get out of control?

AI presents potential threats to humanity. Experts are divided on this issue. A section feels that technology development is unstoppable and

Recently, Bengaluru and Hyderabad airports run by private players have announced that they would have face recognition equipment run on AI for making the check-in hassle free. The Airport Authority of India (AAI) has also said that it will introduce this system in all airports as a part of the Digiseva in a short period of time



in its wake it will bring protective mechanisms for the mankind. An example is nuclear science. There are productive and destructive uses for the nuclear energy. Science will reinvent systems that can check mankind from misusing its powers. This does not mean future R&D on nuclear science should stop. That said, the main threat perceptions of the AI are unemployment, threat to privacy, development of autonomous weapons made of robots, complexity created by proliferation of machines controlling and supporting each other. It may lead to dictatorial regime similar to what George Orwell described in his book Nineteen Eighty-Four. But that should not be a full stop to widen our horizons in the AI, which I believe has more good than bad.

Why and how has IoT entered into the business ecosystem of India, with reference to both consumer and industrial IoT as part of Industry 4.0.

IoT, for both the industrial and the consumer segment, requires technology integration as well as establishing new business models. IoT helps in maintaining quality across the entire ecosystem by almost real-time triggers ensuring a great customer experience every time. IoT has the potential to drastically reduce business costs and enabling new revenue streams.

There is a lot of scope and unexplored opportunities for IoT providers to develop compelling IoT solutions that can explore how the ability to collect and analyse disparate data in real-time. Developments with regards to IoT will play out within and across enterprises. This offers opportunities for sustained value creation and even disruption.

WHY THE TIME IS RIGHT FOR AI-ML BUSINESSES

Companies are mining online sales data to determine what products to make. As the data shows emerging trends, businesses can switch to manufacturing those products

Jitin Khanna
Jaskarn Singh



The footprints of Artificial Intelligence and Machine Learning can be traced back to the 1930s. The pattern continued in the late 1990s, when a confluence of multiple technologies led to the current boom in AI. Alan Turing, a mathematician and computer scientist in the 1950s said that computers could think. He devised a test to determine if a computer could be labelled intelligent.

But during that era, not enough processing power was available for machine learning to take place; therefore the field of AI was only established in 1956 after the inventions of computers. Even then, due to lack of computing power, AI did not deliver on its promises at that time. Also, the issue of language translation is so complex that even today it remains a challenge.

Evolution of Deep Learning

Neural Networks are a form of AI where flow of information resembles the human brain. In 2006, Geoff Hinton suggested stacking of large number of neural networks on top of each other to demonstrate that this technique gave these networks the capacity to learn non-linear relationships and to overcome some of the drawbacks of existing neural networks. Thus, the term deep learning was born.

In 2012, researchers were able to beat top ML models in a famous image recognition challenge called ImageNet. In 2016, Google's AlphaGo AI program beat the prevailing world champion of Go, Lee Sedol. Go, is a famous Chinese board game that

AI became a rollercoaster ride when Google, IBM and other companies started using it. IBM designed an AI called Deep Blue that successfully beat Garry Kasparov, the world chess champion in the 1990s. This event brought AI to the centre stage, and triggered new research in AI and ML

Several technological factors have led to AI resurrection

- * Cloud computing could make 300 graphics processors available for training your AI model in under 5 minutes. The setup can be retired quickly by next morning, unimaginable just 5 year ago.
- * Universal mobile computing for the masses led to more data generation.
- * The Internet has reached to the furthest corners of the globe.
- * Availability of cheap sensors due to IoT spread across manufacturing, mining, and other areas.
- * Cost of storing data has fallen dramatically.
- * Big Data has developed, defined by 3 Vs –
 1. Volume—Everyday, about 2.5 quintillion bytes of data are generated.
 2. Variety—80% of data is unstructured (video, images and sensors, etc).
 3. Velocity—Every 60 seconds, 400 hours of video are uploaded to YouTube.

has more possible moves than the number of atoms in the universe.

Today, AI platforms like Tensorflow feature easy-to-follow tutorials on how to design AI models on our laptop. The vulnerability for AI and ML are data availability and processing power. If a scarcity exists of either, then prospects for AI success are low because statistics does not perform well under low data volumes. Also, if you have large amounts of data, the processing requirements rise.

Each of these factors brought large step changes in the amount of data available worldwide. The issue

Once we can have affordable data lakes and processing power available, we should be able to start developing more complex AI algorithms to extract information from raw data

now is how to make sense of all this data, which is where AI comes. AI and machine learning sits at the epicentre of this perfect storm as no human being can process terabytes of data through the normal methods of drawing graphs in visual tools or writing programs in Excel.

The whole product lifecycle is now being impacted by ML. For instance, companies are mining Amazon and eBay sales data to determine what products to make. As the data shows emerging trends, businesses can switch to manufacturing those products. Pricing these products will need machine learning support. Manufacturing processes can use machine learning to improve the usage of plant machinery and avoid down times.

ML: Use Cases for Modern Enterprises

Few common themes will be apparent while considering use cases for ML...

Negative Aspects	Examples
Time Consuming, repetitive and tedious tasks	Monitoring shelf usage in a store Checking multiple sensors to predict mechanical failure
Tasks prone to human error	Entering invoice data Gathering data from different sources to compile result
Performing critical and real-time Decision-making in a complex and fast changing situation	Instantly re-routing courier to avoid traffic congestion Managing furnace temperature in a mill

Few top use cases for Machine Learning

- True Knowledge: Rio Tinto, one of the world's largest mining companies, installed an AI recently to read and apprehend huge quantities of mining-specific documents archives.
- Risk and Profiling: Banks and insurance companies can use machine learning to develop credit profiles for the customers.
- Robotic Process Automation: Automating resource-intensive activities in an organization. For example, Website scraping, customer order processing, customer email replies, call centre operations.
- Fraud detection: Visa runs a fraud detection check immediately before approving a credit card transaction by going through an enormous amount of data from all customers.
- Campaign effectiveness/forecasting: Machine learning can learn the complex relationships between discounts, seasonality, special events, distance to closest competitor and other variables to arrive at highly accurate forecast.

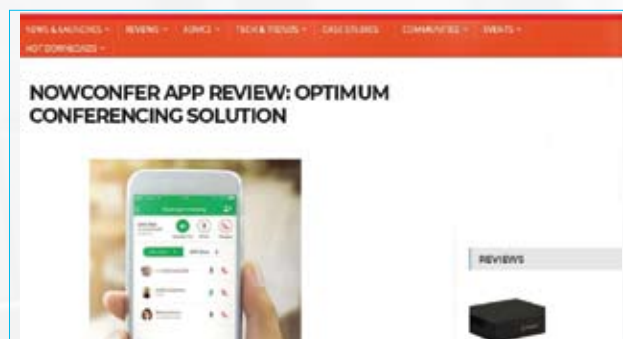
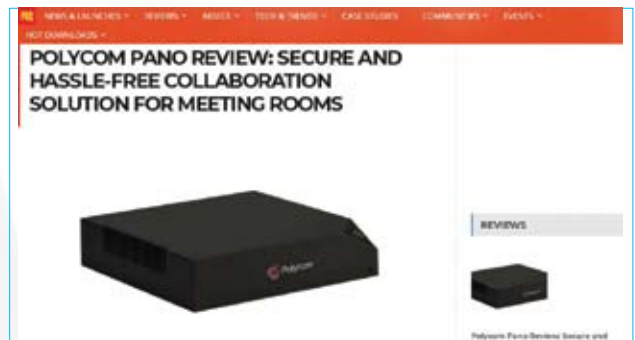
After sale-support now requires machine learning chatbots to support customer all around the clock and using machine learning can reduce the wait times for customers and can be faster than humans support staff. Exceptions are only the handful of industries which are data poor or where the subjective way or flavour of human feelings is involved. For example, people will be hesitant to let a computer cut your hair.

Jitin Khanna is Data & Analytics Architect and
Jaskarn Singh is AI & Data Scientist

PRODUCT REVIEWS

A Powerful Marketing Vehicle

Thousands & thousands of products are launched every year. But a bunch of them are reviewed. A good product backed by experts' review translate into increased user interest and hence sales. Get your product reviewed by CyberMedia Labs which is run by a team of experts/product technologists having 10+ years of experience.



Visit: pcquest.com/reviews/ for more product reviews by CyberMedia Labs

SOME OF THE CATEGORIES CYBERMEDIA LABS SPECIALIZES IN:

• Firewalls	• UTMs	• Thin Clients
• IT Infrastructure Hardware & Software	• Networking Devices	• Printers & MFDs
• Audio Equipment	• Cameras	• Smartphones & Tablets
• TVs & Display	• Computers & Laptops	• Tools
• Games	• Mobile Apps	• Imaging



To leverage the opportunity of product reviews by CyberMedia Labs

Contact us:
Rajiv Pathak
Marketing

marketing@cybermedia.co.in,
+91 8010757100, 0124 482 2222, ext: 219

TECNO PHANTOM 9 REVIEW

What do you expect from a 15k smartphone to offer? The competition in the segment is quite high, every brand has some offering within 15k, but Tecno flame-up the price range with Phantom 9. It is a feature-rich smartphone – triple camera, 6GB RAM and 128 GB internal storage etc. are a few.

The phone looks good and has promising features, but what about the performance, let's find out.

Design

Nowadays, most of the devices come with glossy back, Tecno also used glossy back panel. Beneath the glass, it added a 3D print that adds more beauty to the phone. According to the company, the bottom layer is superimposed with Kevlar's technical sense, which adds to its overall value.

The Tecno Phantom 9 boasts a curved glass-like panel with aurora reflective gradient design on the back that gives it premium looks. The thin phone, 7.75mm thick, is comfortable to hold.

The front looks similar to many, with a dot-notch screen that holds 32 MP front-facing camera and two hidden LED flash. The 6.4-inch FHD+ AMOLED dot-notch display has 600 nit brightness and 403-pixel intensity index. The screen produces vibrant colors with balanced contrast. Colour temperature can be managed using the Eye Care Mode transforms your whole experience of streaming videos and playing games.

The phone has in-display fingerprint to offer a seamless unlocking experience. A symbol of in-display fingerprint appears when you pick up or press the power button. Place your finger at the right spot to access your device securely.

Camera

Tecno Phantom 9 has 16MP + 8MP + 2MP rear AI camera setup at the back. It has F1.8 Night Algorithm 2.0 and quad flash along with AI camera. The combination enables you to capture beautiful images even in low light.

The sunlight images come with a decent amount of details and popping colours. The AI camera takes care of the shooting needs and switches to the required mode. The three lenses capture a good amount of colours and depth in a snap. The bokeh mode takes really good shots, but troubles with focus.

The front 32 MP shooter captures beautiful images. It comes with AR emojis, that comes with high-end devices, enabling you to click images with emoji filters to your face.

Tecno has smartly managed to hide two front-facing flashes on the dew-drop notch, which is somehow almost invisible. This enhances the usability of front shooter for video calls and selfies even in dark.

Performance

Tecno Phantom 9 is powered by a 2.3GHz octa-core MediaTek Helio P35 SoC, paired with 6GB RAM and 128GB internal storage. It comes in the only combination, which seems promising. The phone runs HiOS 5 based on Android 9.0 Pie operating system. The UI is stuffed with bloatware, which can irritate you with loads of notifications.

The phone runs smoothly and loads app quickly, though the processor used here is not top of the line. But screen disappointed

— Ashok Pandey
ashokpa@cybermedia.co.in



Price: Starts at ₹ 14,990

Overall: **8.5/10**

SCORE

PRICE: **10/10**

PERFORMANCE: **7/10**

FEATURES: **9/10**

KEY SPECS: 2.3GHz octa-core CPU, 6 GB RAM, 128 GB ROM, Expandable Upto 256 GB, 6.4 inch FHD+ Display, 16 + 8+ 2MP primary and 32MP Front Camera, Android 9.0 Pie OS, 3500 mAh Li-ion Polymer Battery

PROS: Price, design, plenty of storage, front dual flash, decent camera

CONS: Sluggish performance with heavy operations

us, we experienced glitches sometimes when opening a new app or trying to access the top shortcut drawer.

Phantom 9 can easily handle basic operations including internet browsing, multimedia streaming and social media without any hiccups. For high-graphics intensive apps and games, it won't be able to sustain the top-notch performance. Gamers who prefer PUBG or other high graphics-intensive games would be disappointed with its performance.

Battery

The phone is backed by a 3500mAh battery that let you enjoy have fun for the entire day or more with moderate usage. In one full charge, it was capable to provide power for one and a half day. While watching videos, it can last for more than 4 hours and 27 minutes.

Bottomline: Be it specs or aesthetically appealing holographic design, at this price, this is one of the best smartphones right now. Good camera at both ends, decent battery life, but lags with heavy operations. If you have strict budget, then rather than going for Xiaomi, Oppo or Vivo, Tecno Phantom 9 can be your option.

EARPHONE

CROSSLOOP DESIGNER PRO SERIES EARPHONE REVIEW

Are you looking for a stylish earphone? Crossloop has various choices for you, blended with style. Crossloop Designer PRO Series Earphones, authentic fabric braided earphones are designed for new-age generation, looking for stylish earphones.

Design

Crossloop Designer PRO Series Earphones comes with unique construction – the bohemian design. The unique fabric braided design, are ceased with highest quality braids. It adds beauty as well as gives it more durability than traditional plastic coating cords. It protects wiring from wear and tear plus provides tangle-free experience.

The earphones are designed keeping the new age requirements in mind. It has Noise-isolating design that keeps the noise out and offers great music experience. The earphones are comfortable and the housings are ergonomically shaped. The in-ear housing is angled at 45 degrees that keep it securely fit and not fall out of the ears easily.

Features

Crossloop earphones are compatible with all android phones like Samsung, Oppo, Vivo, Mi, One plus (up to One plus 6), Asus, Lenovo, Etc. & iPhone till 6s. It comes with advanced earplug that fit securely as well gives immersive music experience.

Crossloop earphone comes with an inline advanced microphone. It has the volume rocker and an access button that enables you to answer and reject phone calls, play & pause songs or even skip songs.

The earphones feature noise-isolating ear-buds (3 different size ear tips bundled with the set). It also supports Hands-free calling in between the music with volume control and supports Siri/Alexa/Google activation from the button itself.

Performance

We used Crossloop Designer PRO earphone for more than two



Supports all voice assistants with inline activation button



Price: Starts at ₹ 699

SCORE

PRICE: 9/10

PERFORMANCE: 9/10

FEATURES: 9/10

Overall: 9/10

KEY SPECS: 14.33 mm dynamic driver, TPE Cord, 3.5 mm Audio Jack, Mic & Button

PROS: Balanced sound, bass, perfect fit, stylish design, mic

CONS: None

weeks, and here what we feel about it. The in-ear headphones fit perfectly and as we have already mentioned that it comes with 3 sets of replaceable ear tips so you can choose your perfect fit.

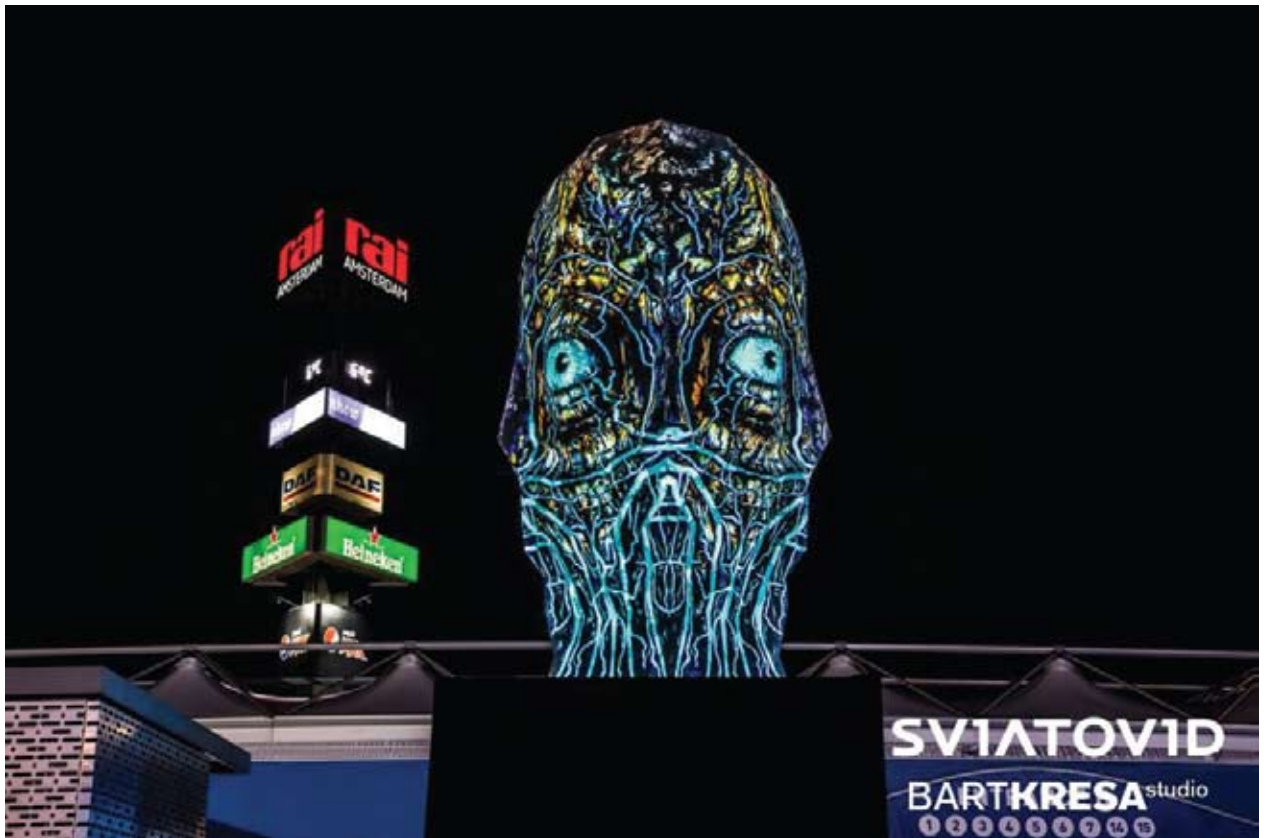
We enjoyed various soundtracks on this, and it performed well. It produces loud and clear sound with balanced bass and treble. While playing songs like Angel of Mercy by Black Label Society, Stadium Arcadium, brutal bass drops, trance music and Bollywood romantic and dance songs, it was amazing. The Crossloop Designer PRO Earphone deliver a balanced sound and its frequency distribution is also well managed. On tracks with intense sub-bass content like Titanium by David Guetta which features dance club style beats, the earphone delivered a great amount of bass. Sia's vocals were clearly audible in between the bass of this electric pop song.

The mic is quite impressive, we used it while riding a bike and the other person was able to get our voice quite clearly. The noise cancellation is also good but has some leakage.

Bottomline: Crossloop Designer PRO Series Earphone has a perfect fit design and well-balanced sound. It is a perfect choice for music enthusiasts looking for a stylish earphone at this price point.

Creating A High-End Transformative Experience

BART KRESA studio is a premiere projection mapping company that specializes in developing one-of-a-kind experiences around the world. Here, Bart Kresa, tells us more.



Tell us more about how you started off in the projection artwork/mapping industry, and how it has evolved over the years for you?

Bart Kresa: I was born in Warsaw, and grew up studying classical music. When I was 21, I moved to LA, and was attending a school of photography. During school, I met a teacher who was creating installations with multiple slide projectors. So, I was already familiar with projections as art in galleries.

I started to develop an interest in photography, and this eventually led me back to projections. In the basement of my first house in LA, I built a small studio with four slide projectors and electronic instruments. Then, I started experimenting.

My first architectural projection piece was in 1995. I was invited to work on a project with artists from San

Francisco and Italy for Arte Multi Visione in Italy. Over the next ten years, my personal art passion developed into bigger and bigger projects.

In 2006, I started my company, BARTKRESA studio, and worked on my first really big project, Gift of Angels, at Universal Studios Japan. Since then, I have travelled the world, worked on many different and inspiring projects. In December, I took a team of more than twenty people to India to create a show that had 90 projectors for a two-night-only event. That was exciting.

In February, I started an academy for projection design in Poland. We have four students from three countries, and I love getting to pass along the knowledge and experience that I have gained. I truly love this medium.

What is the key foundation in the curation process with your clients? How do you piece it with your inspiration and creativity?

Bart Kresa: Our goal is to create a high-end transformative experience, and we never want to settle for anything less. As a philosophy, we challenge ourselves to make every project original. We never want to do the same thing twice. I also challenge myself and my studio to stay on the edge, learn new things, and explore new ideas.

For the last few years, we have been exploring 360-degree projection-mapped sculpture. Our newest piece, Sviatovid, is a 15-foot-tall sculpture that is designed and built with a library of amazing, musically driven animation.

What were the key challenges you faced when setting up these shows, in particular how did you solve outdoor venue problems vs indoors?

Bart Kresa: We have certain power, the Internet, and time requirements for our installations that do not always match the resources present, or the schedule that the client has in mind. As a result, I have developed two production trailers that we take on site with us.



We still need power and the Internet on site, but we try to bring everything else that we need to install and adjust the projections in as efficient and minimally invasive a way as possible. This allows us to work with the constraints of the location, and to be as flexible as possible.

Tell us why have you chosen to speak at InfoComm India 2019, and where do you see major opportunities for projection mapping in this region (South Asia/ Mid-East)?

Bart Kresa: I appreciate Avixa's dedication to bringing awareness to all of the facets within the AV industry. Even though projection mapping has existed for a long time, this medium is still unfamiliar to many people.



BART KRESA, FOUNDER/MASTER PROJECTION DESIGNER, BARTKRESA STUDIO

I appreciate the opportunity to share the artform that I love with my peers.

Both in this region, and around the globe, we are entering into the experience economy. I see projections are the perfect tool for creating unique, immersive experiences. My outlook on our industry is that we are beginning a golden age of projection.

What will be the key takeaway by the audience attending your keynote address?

Bart Kresa: The presentation will give an overview of our studio's approach to design. I will use some of our projects as case studies, showing the application of the history of projection mapping, and principles of design thinking in our development and design process.

Catch Bart's keynote address on "The Future of Immersive Experiences" happening on 18th September 2019.

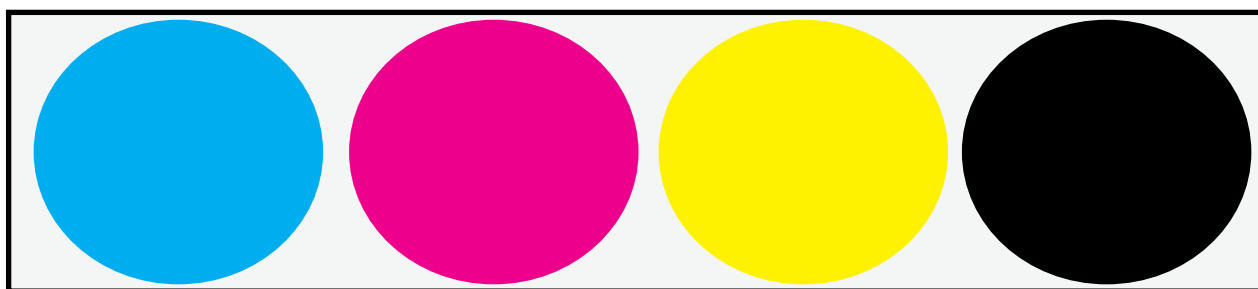
As this is a by-invite only event, kindly RSVP with us at shaziaa@falcon-mail.com

infocomm
INDIA
18 - 20 September 2019
Bombay Exhibition Centre, Mumbai
www.infocomm-india.com

UNDERSTANDING THE INK TANK PRINTER REVOLUTION

Siva Kumar, Senior General Manager of Epson's Inkjet printers, talks about the Ink Tank printer revolution, which has really taken off this decade and how lowering costs have led to a greater penetration into the overall market with eco-friendliness.

Sunil Rajguru
sunilr@cybermedia.co.in



How the ink tank printer took off...

Epson became the first company to introduce the genuine inktank printer in 2011. Before that we had the ink cartridge model, but the inkjet market was not really growing. We did a survey in the emerging markets including India and found that ink cartridge as a concept was not acceptable mainly because consumers did not have the freedom to print. It was very easy to buy the product, say for Rs 3000, but the cost of printing per page in black was about Rs 1.50 and Rs 5 for colour. People also wanted to avoid the frequent refilling of the ink cartridge.

Based on that feedback we introduced the ink tank printer and its acceptance as a technology has grown well. For example before 2011 if it was 100% ink cartridge version, last year ink tank has taken 71% of the space. There has been a drastic reduction in costs and its just 7 paise for black and 18 paise for the CMY colour now.

As far as the ink bottle goes, it gives 4500 pages for mono and 7500 for colour. The combination of high yield ink bottle with low cost of print attracted not only the home user, but also the office customer, that is the commercial segment including SOHO, SMB and corporate segment. Thanks to this we have been able to penetrate these markets and grow our market share.



The success of the mono ink tank printer...

We initially started with colour ink tank, but now we introduced just the mono ink tank printer in 2013. The biggest acceptance of this came from the office segment as most of the printing there happens in black and white. They did not appreciate the colour printer so they wanted us to make the mono version. We currently have 14 models just for that. This has helped us penetrate deeper into the office segment. It was particularly popular with photocopy-printing shops, cyber cafes and students who have to take a large number of printouts for project work.

When compared to a laser printer...

While the ink tank market has grown, the laser printer market has shrunk in the past years. Customers believe laser printers give speed, quality and reliability. But all these factors are covered in the ink tank printers and the prints are water resistant and smudge resistant. But over and above that, ink tank printers have much cheaper printing cost. In fact to cut costs in laser printing, some people go in for a refill toner which leads to a host of other problems. The TCO (Total Cost of Ownership) is also much lower in ink tanks.

Why they are more eco-friendly...

They are also eco-friendly for all the above reasons and they also consume less power. There is also less e-waste as a plastic bottle is much simpler when compared to a laser cartridge. When you look at the physical dimensions, the ink bottle gives a 97% space saving. But we are not just talking about the saving in the office space, but the complete supply chain: From packing in the factory, to transportation to reaching the customer. Then the ink tanks last also much longer.

We are giving this message about sustainable development to all our SMB and corporate customers. Epson has already adopted 13/17 of the United Nations Sustainable Development Goals. (Certain goals like No Hunger, No Poverty, Life under water etc we can't adopt, but all others we can). We have high productivity products that are compact and efficient. They have less e-wastage, less power consumption and less water consumption.

How Epson compares with its competitors on this...

We were the first to introduce the genuine ink tank printer in 2011. Initially everyone thought it wouldn't be a success but later other brands realized that ink tank was going to be the future and they started developing it. The basic difference between us and the competition is that we use the Micro Piezo Technology whereas the others use Thermal Inkjet.

A Micro Piezo printer is much more reliable and it can have a precise placement of dots. It can produce high resolution prints and it can produce variable dots. This means that it can print high coverage images without reducing speed. Even the smaller or finer details will be covered with smaller dots. When it comes to a solid background, then it covers with a big dot. This is called Variable Sizes Droplet Technology (VSDT).

But in a thermal, if a high coverage and finer details have to be reproduced, it uses only the smallest droplet. So to cover up the solid background, it has to print multiple times. That's why it loses out on speed. These are all mechanical parts and that's why the replacement



rate is also high in thermal.

On ease of using the technology...

If you look at our latest generation of Ink Tank printers, we changed the ink bottle design and they are now squeeze-free and spill-free. You just have to place the ink bottle on the ink tank and the ink flows automatically. It is easy to remove and shuts automatically even if there is slight space left while placing.

Long back with inkjet printers, people felt that if it was not used for long, the nozzle would get blocked. We can use an ink pen analogy. When a pen is used continuously, the ink flow is very smooth. But when it is not used for 45-60 days, the flow is not smooth while writing and we try to shake the pen and end up spilling ink. So when it comes to inkjet technology, the printer knows how long it is idle and it goes for an auto cleaning when you switch it on after 45-60 days. The user may not know, but the nozzles automatically recover and start printing. Even in the worst case scenario of nozzle clogging due to dust accumulation, there is a cleaning provision given in the printer driver to rectify that. We are successful in the educational vertical where they have holidays of 30-45 days. The printer is idle during that time but printing is smooth when work is resumed.

Some of the latest innovations...

Over and above that in our latest model we have introduced three more improvements. One is printhead mounted on electro conductive plastic which protects the nozzle by not absorbing dust that may have accumulated on the paper. Two, we developed an advanced tube which minimizes bubble formation. Third, the ink drying itself is changed. On top of that we have things like auto cleaning when the printer is idle.

Finally these ink tanks are both economical and eco-friendly.

Subscribe To PCQuest To Know More About Latest

- Tech Products
- Gadgets
- Product Reviews



4 EASY WAYS TO SUBSCRIBE

1. Visit: subscriptions.cybermedia.co.in/pcquest.aspx

2. Through Cheque/DD in favour of 'CyberMedia (India) Ltd'

3. Bank Transfer via RTGS/NEFT

Bank Details: ICICI Bank Limited, A/c no. 017705000132, Branch & IFS Code: Gurgaon, ICIC0000177

4. Call: 0124-482-2222

For any subscription related query please email: rsepcquest@cybermedia.co.in
Digital subscription available on Magzter, Readwhere, Readly, Wink & Paperboy.

Yes!

I want to subscribe to PCQuest



	Period	Issues	Price for New Subs.	Price for Renewal	Your Benefit Zone
☐	1 year	12	Rs. 1500	Rs. 1350	Save 10% on renewals
☐	2 years	24	Rs. 3000	Rs. 2700	Save 10% on renewals
☐	3 years	36	Rs. 4500	Rs. 4050	Save 10% on renewals

Please tick your subscription choice above, fill the form below in CAPITAL LETTERS and mail/fax it to us.

☐ I want to avail premium service of receiving my subscription copy by courier. Tick which ever is applicable.

☐ ₹500/- 1 year, ☐ ₹950/- 2 years, ☐ ₹1400/- 3 years

Name: Mr/Ms _____ Date of Birth:

Organisation: _____ Designation: _____

Delivery Address: _____

City: _____ State: _____ Postal Code:

Mob [+]: Tel: Email [+]: _____

☐ I am paying ₹ by DD/Cheque No.: Dated:

Payable at (specify bank and city) _____

OR

☐ Please Remit for ₹ Through RTGS/NEFT to our A/C details given below:

Bank Name: ICICI Bank Limited A/c No. 017705000132, Branch & IFS Code: Gurgaon, ICIC0000177

[+] Essential fields

Signature _____ Date: Subscription No. (for renewal) _____

Order can be faxed to:

0124-2380694 or mail the form with payment (cheque/DD) to:

Sarita Shridhar, Cyber Media (India) Ltd, Cyber House, B-35, Sector 32, Gurgaon - 122001 Tel: 0124 - 4822222.

Terms & Conditions: _____

• This special offer is valid for a limited period. • Rates and offer valid only in India. • Please allow 4-6 weeks for delivery of your first copy of the magazine by post & 8-10 weeks for delivery of your assured free gift. • Send crossed Cheques in favour of Cyber Media (India) Ltd. • Please write your name and address on the reverse side of the cheque or DD. All outstation cheques should be payable at par. • Cyber Media (India) Ltd. will not be responsible for postal delays, transit losses or mutilation of subscription form. • Cyber Media (India) Ltd. reserves the right to terminate or extend this offer or any part thereof. The decision to accept or reject any or all forms received is at the absolute discretion of the publishing company without assigning any reason. • Please include pin code for prompt delivery of your copy. • In case payment is through credit card, date of birth must be mentioned. • Request for cancellation of subscription will not be entertained once the free gift has been dispatched. • All disputes shall be subjected to Delhi jurisdiction only.

IOT AND SMART HOMES HAVE MULTIPLE APPLICATIONS IN THE INDIAN MARKET

Dr. Narendra Bhat, Founder & President of BuildTrack, a Smart Automation Building Management Systems (BMS) company, explains how smart technology can be applied in homes, hotels, hospitals, enterprises and even in the rural market

Sunil Rajguru
sunilr@cybermedia.co.in



What is the status of smart automation and IoT in India and which are the sectors that are proving to be the early adopters?

Smart Automation and Internet of Things are both technologies that are rapidly gaining acceptance in the Indian market place, especially with the rapid rise in the number of mobile devices with Internet access. These technologies are being deployed in situations where

control of electrical devices and monitoring of sensors is required especially from remote locations and over smart apps using devices such as smart phones and tablets.

BuildTrack's experiences across India in both metros and smaller cities suggest that the key sectors in which there is uptake of solutions include Home Automation, Guest Room Automation and Work Management in Hotels, Building Management Systems

for Commercial Buildings, Energy Efficiency Systems in Offices and Nurse Call Systems in Hospitals and Senior Living.

What is the difference between implementation strategies in the home and enterprise domains?

The differences between home and enterprise may be more visible in terms of the nature of usage, rather than the deployment itself. In both situations there are the same products that enable the automation, i.e. gateways that connect and listen to nodes and sensors, with the nodes usually located behind switch panels and connected to the switches and the sensors being distributed across spaces as per their application. The gateway also connects to the internet or to a local network, depending on the need of the home or office owner to access the control and monitoring when away from the premises. The control is usually for lights, fans, ACs, curtains/blinds, in both situations, but in homes it can extend to TVs, STBs and media devices.

Can you comment on your Energy Efficiency and Building Management Systems (BMS)?

BuildTrack's Energy Efficiency systems are usually in the form of wireless sensors that communicate to and control lights, fans or ACs. This control is facilitated through nodes that are connected to these devices, and to which the sensor communicates to

The implementation strategies are different based more so on the nature of the solution being wired, wireless or hybrid. This is dictated by whether a new building/renovation where wiring and civil work are underway or a retrofit situation where neither are possible. The size of the campus or facility (or home) can also make a difference in the choice of deployment. In the case of wired solutions, the conduit locations must be determined, whereas in the case of wireless the availability of signal strength and the location of the routers make a difference to the implementations



DR. NARENDRA BHAT
Founder & President
BuildTrack

either turn these devices off or on as the occupancy of the space being monitored changes. These can be deployed in aisles, cabins, bathrooms, pantries, conference rooms, stairwells, parking areas and more to conserve energy. They operate autonomously without needing access to a network or needing Apps etc. Our various systems and solutions have twice been awarded by CII with the 'Most Innovative Energy Efficiency Solutions' within the last 4 years.

Building Management Systems on the other hand, work by actively controlling, monitoring or scheduling the various devices or sensors in the building. These could be motors, pumps, elevators, security barriers and other such devices. The sensors can be smoke, gas leak, intrusion, laser perimeter monitoring, air quality and other such. Cameras and network video recorders can also be integrated to BMS systems to provide a single point of control that enables management of all devices in a building. The use of Internet of Technology solutions in this area, by BuildTrack is unique in the world and has also been recognized by a prestigious award from the Internet and Mobile Association of India (IAMAI) in 2018.

Can you tell us about your wireless, wired plus hybrid solutions and when which is required?

BuildTrack's wireless solutions are mostly intended

for retrofit situations where any type of electrical or civil work is not possible. The nodes used for control are sized to fit, invisibly, behind any of the existing switch panels, even as small as a single switch panel. The sensors are also wireless. The gateway can also connect wirelessly to a router, thereby enabling a complete wireless deployment for finished homes, hotels, offices etc.

The wired solution by contrast has a single thin cable that loops through the property and is used by the gateway to communicate with the nodes. The nodes for wired and wireless situations are similar in size and capability.

Can you comment on some of your successful implementations and their uniqueness?

In the areas of Home Automation, we serve many builders such as Lokhandwala, Kalpataru, Puranik and Godrej for entire buildings. We also serve multitude of individual homes ranging in size from small 1 BHK to mansions which have over a dozen bedrooms.

Our systems also are deployed to serve as the Building Management System for 'The 42' which is the tallest building in India, and we enable it to also be one of the smartest through the deployment of our solutions.

In the areas of enterprise, we have served companies such as Jaguar Lighting where several of their customer orientation centers across India are using our IoT technology and our Smart Apps to delight the customer, when they are present in them. We also serve companies like Bridgestone, Mazagaon Docks, GM and Ramada Hotels.

How much of a role does AI play in your solutions and what are the expected future breakthroughs?

Currently AI plays a role in our solutions in checking on the health of our IoT systems that are operational. We anticipate expanding this to serve other predictive maintenance needs for many essential assets and electrical devices used in homes and

Wired solutions are ideal for new and spaces being renovated. There is more reliability in wired solutions as they are not dependent on wireless signal strength that can be influenced by outside issues

Both the control and monitoring are used typically to deliver benefits in the areas of—

Safety: Through alerts for smoke and fire, cooking gas leaks, Carbon Dioxide levels

Security: Door intrusion, window glass break-ins, motion sensing

Comfort: Control of lights, fans, ACs

Conveniences: Control of TVs, media devices, curtains and blinds

Energy Efficiency: Automated shut-offs based on occupancy or pre-set schedules for all energy consuming devices like lights, ACs. Monitoring of energy consumption via Smart Energy Metres

Operational Efficiency: Centralised control or monitoring of all assets in a building such as motors, pumps, elevators, water tank levels, fire panels, fire pump pressure etc.

enterprises.

More so than AI which is still nascent, the use of voice technologies from Amazon and Google, and integration with these solutions is creating new areas of breakthrough. These are rapidly gaining interest and popularity in Home Automation, Hotel Guest Room Automation and also in Hospital Rooms.

Can the rural market and villages adopt IoT solutions? How can the government play a big role in that?

In the rural markets, IoT can play a solution primarily to serve in the areas of safety, security, energy efficiency and even agricultural productivity. Sensors can be used for most of these instances to serve a number of these needs, even without the use of Internet, through local networking with the nodes, these sensors can trigger equipment. For instance, soil sensors can monitor water levels and trigger pumps, motion sensors can trigger security alarms in homes or storage locations.

DIGITAL DISRUPTION, AI AND IOT IN CRM

Colleen Berube, CIO, Zendesk, talks about Customer Relationship Management solutions, how small and large companies should deal with them respectively and also the future that is shaping the industry

Sunil Rajguru
sunilr@cybermedia.co.in

What are the main things that businesses should take note while implementing CRM solutions? What are the common mistakes that they make?

When companies start putting systems in place, they think about the processes they want to automate. They will very often take a sort of inside out perspective. They think about it from running their department point of view or the process point of view. However, given the way that technology and markets have evolved, it's really important at this point in history to truly put the customer first.

Companies need to start with the questions; what kind of an experience do I want my customer to have? What are they, given the kind of company that I am, and the kind of interactions that they're going to have with me? My experience is that a lot of companies talk about providing a good customer experience, but very often will make the mistake of not stepping outside their own enterprise and their own internal thinking.

Further, companies should plan for success. Even if you start small, assume that you're going to do well and think a little ahead. Maybe today you're only operating in a country or two. But a global mind set will help you make sure that as you get to the point where you do need to scale, you'll be prepared to do that. This is one of the ways that utilising a service like Zendesk, a SaaS solution, can help you buy some of that global thinking and scalability by taking advantage of our technology.

Moreover, focus on open and flexible platforms due to fast-changing technology. The only thing a CIO can be sure of is that there's going to be a new



COLLEEN BERUBE
CIO, Zendesk

technology, and it's going to be better than the last one. The trick today is to put oneself in a position of being able to move quickly as things change.

I was just listening to someone from Forrester and they were talking about how companies have

to continue to improve the customer experience just for it to be okay. Everyone is consistently raising the expectations with the customers. If you're not improving, you're going to drop behind.

If you look at the companies that are disrupting the market, the ones that are successful are the ones that have put the customer at the centre. If you're a digital transformer and you do not truly make that transition, you will not survive.

How do small and large companies approach CRM?

Sometimes smaller companies can think that they're too small to get something that's a little more tailored to business. On the flip side, large companies can think that they have to pay a dramatic amount of money to implement CRM successfully. Neither is really true. At Zendesk we have a very customisable solution. I think one of our key differentiators in the market is that it's truly easy to implement. It takes a fraction of the time that some of the larger platform companies might take to implement. It costs a fraction of what they might cost. We're really challenging others in terms of that traditional thinking about assuming you have to spend large amounts of money and time to implement CRM.

Also, when you're a larger business, you tend to naturally have a little bit more complexity to your business. Or maybe you have more products and services. Maybe you have a broader geographic span. You tend to have more departments that are specialised. By nature, there will be a bit more complexity to implementing CRM. In addition to that, you're more likely to use other technologies that need to connect. So, there is a difference. But the concepts are the same.

I'm also going to add something that sounds somewhat contradictory to that. On the one hand so many companies when they're starting with us go in for something hugely sophisticated and complex,

To be able to connect the data that's coming from all the different touch points that your customer has with you. Your ability to bring that information together seamlessly and gain insights from it and make it actionable is the key to creating this amazing customer experience

There's a lot of conversation these days about computers taking over the world. Where we are today is that so many businesses just don't even have the possibility to staff 24X7. This is one of the first areas where AI and ML can really help

even if they're not doing some of the most basic things. For example, if you're trying to sell a product to your customers and they already have it, it doesn't require an AI to figure that out. So it's better to start simple and build up the expertise in the context of your customer and getting more sophisticated in the process.

What about chatbots, AI and their future roles?

There's a lot of conversation these days about computers taking over the world. Where we are today is that so many businesses just don't even have the possibility to staff 24X7. This is one of the first areas where AI and ML can really help. It gives you the ability to automate so many simple requests. We find that, even if you look at the AI that our customers use in our products, that customers are able to resolve an issue using our AI solution.

One of the fascinating things about this space is that if you ask people whether they want to have a human interaction, nearly three-quarters of the time they will tell you yes. But the truth is they don't want to. They really just want to get their problem solved. The numbers are much higher when people can quickly self-serve on the answer. This is where the opportunity is. But from both a customer experience perspective and a business perspective there is also the human interaction for where it matters the most. For example, there are those moments where there is that human connection that really leaves a lasting impression on the customer.

What about the Internet of Things and predicting problems early?

If you think about what makes up a customer experience, there's a physical device involved, whether it's a car or a washing machine or the refrigerator. The experience that you're having with that device is part of your experience. One of my favourite sayings is: if you get to the point to where

you have a customer support ticket, it's already too late. You already had failure in your product or service. It's not only a process of effectively managing that customer experience reactively, but starting to think how we can be more proactive.

Our new Zendesk Sunshine platform allows customers to bring together their information about the customer experience from their Zendesk products with other sources they have, including IoT data as well. It runs on AWS and it's built with open standards. It has three main components: Objects, events and files. It's like, what do you know about the customer? What do you know about objects that might be related to them? That could be their washing machine. Or it could activities that have already happened. They give you a pretty universal way of connecting data, and finding all the relationships and the patterns that matter.

In terms of an IoT example, let's take a scooter company service. You can rent these scooters by flashing your smartphone or stick a credit card in and then return it when you

want. Imagine a scenario where someone has left it where it didn't belong, or maybe there's a failure in the wheel or something else is happening. Now that scooter company would really like to know if there's something going wrong with that scooter, particularly if it's rented out at the time. They can get information from the customer who's renting it, but there's also the information that's coming from the scooter through its IoT device about what's going wrong and where it's located. The company can now proactively let the customer know that they need to trade it out for another if something is wrong.

There is more data than we have ever had. But there are better tools than there ever have been to analyse that data. It gives you a much more complete view and looking across your customers you can discern patterns that you were never able to discern before, which will put in a much better position to anticipate what their customers need. Customers would really like for more companies to be proactive to anticipate their needs, but very few companies are actually at that point of maturity and sophistication.

What about the integration of the myriad of social media platforms?

It's the consumers' choice which of all these social media platforms they want to interact with. Part of your job as a business is to give people that access and the channels that they want to be on rather than for the channels we provide. We just recently launched integration with WhatsApp's business API. We're trying to open up more and more opportunities for our customers and to their customers. We recently acquired a company called Smooch that provides interaction with many of these messaging platforms. We're excited about the way that that expands channels that customers can use to interact with.

Regardless of how your customers interact with

you, it could be a phone call, it could be an email, it could be through WhatsApp. What you really want to do is to bring that information together in a cohesive way. So, when interacting with your customer, they can see the full context of the interactions. Let's say you call because you have a problem with a product and they don't know that

I think that we will continue to see a lot of evolution in the AI space and it will become more sophisticated. We will find more and more ways to better satisfy customers with it. But I think the people's desire to have that human touch at the right moments will remain

you also Tweeted or they don't know that you sent an email, because they've got their channels completely segregated. Then they're not combining that to the benefit of the customer. Zendesk does a really fabulous job and gives you the possibility of bringing that information together in a really effective way.

What are some of the things that CRM companies should take note of in the future?

First, there is an ongoing wave of digital disruption and customer expectations continue to rise. There's a declining trust in brands. Companies have to start thinking about building these skills and have the right tools at hand, in order to be able to become much more customer-centric. Second, customers are going to more and more want to see that proactive engagement and companies need to take advantage of the data and the technology. Third, companies will have to leverage AI to drive customer experience starting with the simple things and moving to be more sophisticated over time, so that customers can self-serve as much as possible.

THERE IS A GREAT SHIFT FROM MULTICHANNEL TO OMNICHANNEL

Businesses in India want to adopt technology which is open and flexible. Indian customers are willing to adopt technology and willing to pay a price for it too, explains KT Prasad, Country Sales Director, Zendesk

Sunil Rajguru
sunilr@cybermedia.co.in

Do you see any difference in the Indian market in the way it adopts CRM solutions?

From an Indian perspective, I think we have not changed any product or any of the needs. The global and local needs are very similar. Because I see even the customers in India want to be driving the customer-centric approach, whether it's the digital natives or new companies like Ola, or old businesses and traditional companies like ITC. They see how digital disruption can affect the industry and the businesses. Now maybe in Ola because it's completely digital native, you brought in a CRM system and you put in one system for all. In larger companies and enterprises, when you bring in a CRM, they might have other solutions working in silos.

There are open and flexible solutions we have to offer. You can plug-and-play your voice technology. You can plug it into technology or your business

There are open and flexible solutions we have to offer. You can plug-and-play your voice technology. You can plug it into technology or your business applications to really have a customer conversation and drive relationships

applications to really have a customer conversation and drive relationships. Those are things which we have seen differently. We do not need to make any changes to a product except the call solution.

India is highly regulated for calling. So we partnered with local partners who can provide the voice technology. When a customer looks at it, they look at voice. They look at chat or email or any social channels or a messaging platform. So the voice technology is what we partner in India, but when it comes to the rest, the customer gets to use the complete suite of products.

Has the Indian market been particularly difficult to crack? Are Indian companies willing to pay for such solutions?

What we've seen is that businesses in India want to adopt technology which is open and flexible. I think if you look at the traditional software, then you sell the software and disappear. But from the SaaS perspective, we look at the long term value of a customer. We look at the customer as being at a churn risk. A customer can actually sign up for a month, or maybe for a year, or you can stay for longer. So he has so many options with them. The onus is on companies like Zendesk to provide innovation and really compelling technology that can make a difference to the customer experience.

Because of those approaches, it's been working beautifully for us. We have not seen any resistance. We hear that India is a price sensitive market. But it



KT PRASAD
Country Sales Director
Zendesk

was probably applicable in the olden times. In the new times, if you can drive business value and if you can improve customer experience methods for the business, customers are willing to adopt technology and willing to pay a price for it too.

What are the Indian trends for CRM?

Many Indian trends are similar to global trends. But most customers and businesses in India are moving towards omnichannel, and they will definitely see how it is different from multichannel. The customers are integrating all the messaging technologies like WhatsApp. In fact WhatsApp has been very revolutionary in India. We have 400-500

million smartphone devices, growing at a very rapid pace. Most of the telecom companies today offer data at a fraction of the cost. At \$2 a month, you get unlimited data that consumers are struggling to spend.

Consumers are spending more time on social platforms like WhatsApp, Facebook and Twitter. Customers have a voice today. Earlier, the consumer could send you a business email or make a phone call. But today they can go straight to Twitter. So it becomes important for businesses not to see their brand to be dampened. You want to make sure that the customer experience is constantly increasing. AI is also playing a role.

We are advising customers to use simple knowledge base that is a foundation to really create a great AI experience. But some of the businesses are in a hurry to put in bots. But some of them don't have their foundation right. So we see them coming back and asking about the right path for them. They can then use bots-AI-ML to self-service customers.



The voice technology is what we partner in India, but when it comes to the rest, the customer gets to use the complete suite of products

ARE COMPANIES HIRING SOFTWARE ENGINEERS ALL WRONG?

Software has eaten the world – car companies and banks now compete on the quality of their software tools, and whole industries are undergoing disruption. Certainly, technology is a big part of this digital transformation, but none of this is possible without people with the software development talent to make it happen. It is no surprise that the competition for tech talent is stiff: NASSCOM predicts the AI, Big Data Analytics talent gap to grow from 62,000 to 1,40,000 over the next three years

Raj Sundaresan



If we look at the software engineers' recruitment landscape, it appears that there is a lacuna in the talent available and in the recruitment process. So, if digital transformation is so important and technical talent so hard to find, why do companies go

about hiring software engineers all wrong?

The Lacuna

I've seen it happen in dozens of companies. They bring in candidates, put them in a room, give them

a coding test, and tell them they have 45 minutes to complete the code. Perhaps they ask them to find an answer to an absurd and even unsolvable problem. This is meant to be an assessment of a candidate's technical and problem-solving skills, which is a good goal, but nothing about these artificial tests predicts how the candidate will actually perform in a real world work environment.

We all have this image of a software coder as a loner, working at odd hours doing things that no one else can understand. The reality is that software engineering and coding is a team effort, with lead architects, project managers, and a repository of code where work-in-progress is shared by a team of developers.

Yet, when companies are assessing candidates, they make the engineers work alone and prohibit them from using any reference sources, as if the assessment was some sort of school exam. The working world is nothing like school, so why test people that way?

The Assessment Process

When Altimetrik assesses software engineering candidates, we strive to put them in a situation that's as close to an actual work environment as possible. We call it Playground Exercises for Talent Assessment, and interaction and collaboration are encouraged during the exercise. The word "playground" connotes a sense of fun, putting candidates immediately at ease. The exercises are fun, and candidates tell us they enjoyed and even learned from the experience.

The candidates get a use case to work on, something specific to the industry they will be working in, and they are tasked with finding a solution. They're encouraged to talk and chat with each other, use Search engines and other online resources, and then

Far from having to recall everything from memory, the first step for solving any software development problem is to use Search engine platforms. Why reinvent the wheel when you can find the plans for it on the Internet?

The work is collaborative in nature, so we create an environment that assesses someone's ability to collaborate. What we are really looking for in these sessions is how an engineer works with colleagues. Does he or she contribute to the success of others? When solving a problem, do they get pulled down into a rabbit hole and never come out, or do they know when to seek help?

code on their own and ultimately present the results of their efforts. We have senior engineers, which we call coaches, walking around helping candidates. The coaches are not there to judge or assess the candidate, just to help them think through any difficulties.

The quality of the code counts, but what we are looking for goes beyond just quality code. Are the candidates thinking not just about coding but also about unit testing and whether the code will work as a piece of a larger whole? Those are the types of attributes we need in software engineers, who don't just work on one problem in isolation, but work as a team, leveraging each other's efforts to solve a bigger problem.

As companies strive to rethink their business and undertake digital transformation, they should also look to transform the way they onboard talent. How something is done matters in a team environment, and that is what needs to be evaluated in our hiring processes. I would gladly take three adequate engineers who are great collaborators over four or five great engineers who don't work well with others.

As with the playgrounds of our youth, our Playground Exercises for Talent Assessment explore whether candidates know how to play well with others. After all, you learn more about a person when you interact with them than when you make them take a standardized test.

The author is Chief Operating Officer, Altimetrik & CEO, Davinta Technologies.



October 2019

V&D 25 YEARS

Are you part of "Annual Communication Industry Survey"?
Across Segments

- Network Services
- Network Infrastructure

Analysis of "Top 10 Telecom Companies"

Network Services

Voice

- ☒ Wireline
- ☒ Mobile/Wireless
- ☒ Internet Telephony

Data

- ☒ Wireline Broadband
- ☒ Mobile/Wireless Broadband
- ☒ Enterprise
- ☒ VSAT

Other Services

- ☒ Multi-system Operators
- ☒ OTT/IoT/VAS/mWallet/mCommerce



Network Infrastructure

Carrier Infrastructure

- ☒ Carrier networking: Optical & Converged
- ☒ Core & Access Equipment
- ☒ Passive Infrastructure: Telecom Towers, OFC, Power Solutions
- ☒ Managed Services
- ☒ Test & measurement
- ☒ OSS/BSS
- ☒ Software, Solutions & Consulting

Enterprise Communications

- ☒ Enterprise Networking
- ☒ Structured Cabling
- ☒ Communications Equipment & Devices: Desk Phones, PBX Systems
- ☒ Software & Applications: Conferencing and Collaboration

User Devices

- ☒ Mobile Phones
- ☒ Data Cards
- ☒ Tablets

Participate in V&D 100 Survey

Last Date of Advertisement Booking : 25th September 2019

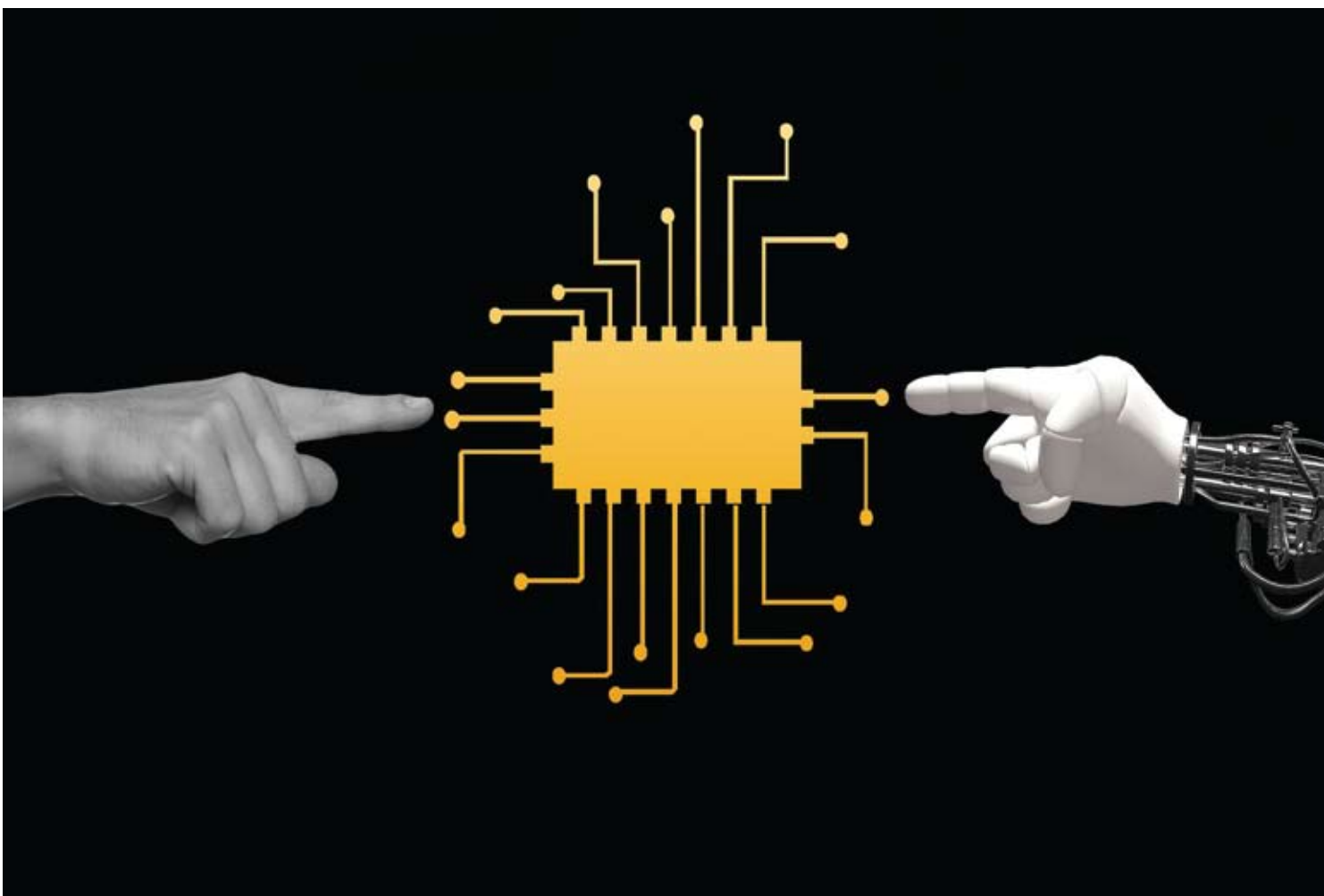
Contact us for customised partnership opportunities

Marketing: Rajiv Pathak | rajivp@cybermedia.co.in | +91 8010757100

WHY INDIA'S MANUFACTURING SECTOR NEEDS AI

India's manufacturing segment can't continue to follow their traditional, Industry 3.0 based processes anymore. Digitization of data is a must followed by identifying the right AI solution to act on it

Anil Chopra
anilc@cybermedia.co.in



The Good News

India's manufacturing sector has been steadily growing thanks to growing Foreign Direct Investments, Government of India's initiatives like Make in India, reduction of Income Tax for companies with up to Rs 250 crore turnover, among others. According to IBEF (India Brand Equity Foundation), the Government of India's objective is to increase the manufacturing sector's contribution to 25% of the country's GDP by 2022 and also create 100 million new jobs in the process. This dream run can only continue if the manufacturing sector also starts embracing next-gen technologies like AI (Artificial Intelligence), to combat its existing hurdles. Unfortunately, India's manufacturing sector still has a long way to go in AI adoption as compared to other sectors. Only a small percentage of companies have actually deployed AI, while a majority either have their plans mostly on paper, or don't have any plans at all.

The good news however is, that AI can have a significant impact on India's manufacturing sector and in fact, there's a strong need for it, according to a recent CyberMedia Research (CMR) survey of large manufacturers. The main thing is to understand the key challenges and then identify the right AI solution that fits the need.

The Way Forward

One common challenge most manufacturers face is to get the right data from their plant's machinery to feed into an AI system. Machinery is typically a capital-intensive investment, so unless you're setting up a greenfield manufacturing plant, chances are that most of your machinery would be many decades old and would therefore lack sensors and

network interfaces to send data over the network to a common application. Being able to add such interfaces and sensors so that the data can be digitised is therefore the first step to an AI journey.

The next step is to be able to do the integration between plant machinery and an AI system. Currently, according to a CMR survey, the manufacturing sector feels that there's a lack of solutions to do this, and it's even more challenging to choose the right AI vendor from the available ones.

Another point to understand is that one size doesn't fit all when it comes to AI. The solution has to be devised keeping in mind every organisation's specific pain points. So start by identifying the key hurdles unique to your organisation before identifying AI based solutions to overcome them. What are required here are efforts on both sides. Manufacturers should start small and then grow as they taste success. Vendors need to create more awareness about their solutions at a sub-vertical level. Everybody for instance, understands how AI can help manufacturers, but how does it help say a textile manufacturer is very different from how it benefits auto-components manufacturers. Use cases at a sub-vertical level are therefore missing, which is something that vendors need to work on, by possibly identifying similar global ones.

Rising raw material costs, declining margins and stiff competition are some other common challenges that every manufacturer faces. On top of that, customers now demand greater customisation with reduced lead times. Being able to control costs, improving supply chain efficiency and enhance production efficiency is therefore a constant endeavor in manufacturing. AI can play a key role here as well. What's required is to identify the right use case and build an ROI model around AI for it. A lot of plant machinery for some manufacturers for instance can be very costly to cold-start if it shuts down. If an AI solution could predict its failure well in advance, then the cost of shutdown could be enough to cover the cost of the solution. It's best therefore to identify how AI can help your business.

The bottomline is that India's manufacturing segment can't continue to follow their traditional, Industry 3.0 based processes anymore. Digitisation of data is a must followed by identifying the right AI solution to act on it. The government is also supporting AI adoption by bringing out an AI policy, conducting workshops on AI for MSMEs, etc.

What's required is for the manufacturers to take cognizance and start moving forward.

While the onus will be on the individual initiative to keep upskilling oneself, even enterprises and the government will need to intervene and strategise on how to enable an AI-inclusive world

INDUSTRY 4.0

INSIGHTS | BEST PRACTICES | TECH ROADMAP

20 September 2019, New Delhi

- Full day conference, modelled as an "Industry transformation collective"
- 5+ Practical industry sessions
- Thought-leading speakers
- Annual congression of 150+ IT leaders and decision makers

Focussed Areas



Artificial
Intelligence



Machine
Learning



Industrial
Automation



Real-Time
Data



Supply Chain
Management



IoT



Logistics



e-Commerce



Manufacturing

Award Categories



Plant Automation



IIoT



Innovation



Smart Factory



Smart SCM

Contact us

Marketing & Alliances

Rajiv Pathak

rajivp@cybermedia.co.in | +91 8010757100

dqconclave.com

Rittal – The System.

Faster – better – everywhere.

SWIFTEST PRODUCT DEPLOYMENT TO ADDRESS BUSINESS NEEDS FASTER

FOR BUSINESSES WHO PREFER
NOTHING BUT THE BEST

GERMAN ENGINEERING

INDIA SPECIFIC EXPERTISE

GLOBAL STANDARDS



At Rittal India, we believe in providing superior and expert solutions to suit all your needs. With our ability to swiftly deploy effective solutions coupled with our industry specific expertise and cutting-edge products, we enable you to address the demands of your business faster, better, and everywhere.



+91 93424 12004



info@rittal-india.com



rittal-india.com

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

