INDIA'S LEADING IT MAGAZINE WWW.EXPRESSCOMPUTER.IN @ExpComputer.

AN INDIAN EXPRESS GROUP PUBLICATION VOLUME NO. 29, NO.12, PAGES 12, DECEMBER, 2018, ₹75

EXPRESS COMPUTER

6 | SPECIAL FOCUS: Enterprise Security

8 | FEATURE

BSE goes live with deception technology

10 | INTERVIEW

Shibu Paul, Regional Sales Director – APAC, Array Networks

11 | EVENTS

Customer-centric organisations look at AI, ML and bots to enhance client experience

SBI STEPS UP DIGITAL ACCELERATION WITH YONO

In its bid to become one of the top 10 digital banks in the world by 2020, SBI is banking heavily on this single, unified platform which is being used for end-to-end customer acquisition

EXPRESS COMPUTER

DIGITAL NORTH EAST

CONNECTING THE UNCONNECTED

Microsoft

PRESENTS

NORTH EAST Technology Sabha

An Express Group Initiative

INDIA'S LEADING E-GOVERNANCE SUMMIT

NOVEMBER 23-24, 2018 GUWAHATI, ASSAM

GOLD PARTNER

Schneider Electric

THANK YOU!

The Indian Express Group thanks all our delegates, speakers and partners for their support in making Technology Sabha a grand success!

HOST STATE PARTNER: Digital India Power To Empower | অসম চৰকাৰ Department of Information Technology Govt. of Assam | AMTRON

PRESENTING PARTNER: Microsoft

GOLD PARTNER: Schneider Electric

DIGITAL ACCELERATION PARTNER: Hewlett Packard Enterprise

CLOUD TECHNOLOGY PATNER: ORACLE

ARTIFICIAL INTELLIGENCE PARTNER: aws | intel

ANALYTICS PARTNER: sas

VIDEOCONFERENCING PARTNER: Polycom

DIGITAL INNOVATION PARTNER: SAP

NETWORKING PARTNER: JUNIPER NETWORKS

MOBILITY PARTNER: SAMSUNG

CYBER SECURITY PARTNER: FORCEPOINT POWERED BY Raytheon

DATACENTER & CLOUD INNOVATION PARTNER: esds enabling futurability..

TECHNOLOGY PARTNER: KASPERSKY lab

PARTNERS: SONICWALL | Panasonic | PEGA

AIRLINE PARTNER: IndiGo

60+ HIGH PROFILE ATTENDEES | 2 DAY RESIDENTIAL CONFERENCE | TECHNOLOGY SHOWCASE | PRESENTATION SLOTS | POWER DISCUSSIONS | MEETINGS

WITH DIGITAL LENDING RISING FROM US$ 75 BILLION TO US$ 1 TRILLION BY FY23*, CAN YOU AFFORD TO MISS YOUR BIGGEST OPPORTUNTIES IN 2019

Munish Mittal
CIO, HDFC Bank

Shiv Kumar Bhasin
CTO,SBI

Sanjay Narkar
CTO, IDFC Bank

Hackathons. Loans delivered within minutes. Chatbots. AI. Machine Learning. Digital Only Banks. Automations of almost every process. Express Computer understands this huge digital shift in the BFSI sector, and has hence conceptualized the **BFSI Technology Conclave** – a conference that will witness India's foremost thought leaders and influencers. This is the fourth edition of the conclave.

TOPICS TO BE COVERED:

- Lessons and perspectives from transformational digital leaders
- Open Banking, Next Generation Chatbots and startup partnerships
- A status check on Artificial Intelligence and Blockchain
- Hackathons for improving competitiveness
- Enterprise Security: How to proactively protect your company in a digital era

PAST SPEAKERS:

Munish Mittal, CIO, HDFC Bank
Shiv Kumar Bhasin, CTO,SBI
Nitin Chugh, Country Manager, Digital Banking, HDFC Bank
Tapan Kumar Singhel, Managing Director & CEO,Bajaj Allianz General Insurance
Samrat Das, CIO, PNB MetLife
Ashwin Khorana, CTO,Janalakshmi Financial Services
Dr A S Ramasastri, Director, IDRBT

EXPRESS COMPUTER

BFSI TECHNOLOGY CONCLAVE

JANUARY 18-19, 2019 PUNE

WHY PARTNER

- Engage with 100+ key decision makers
- Establish your position as Thought Leader
- Leverage a well co-ordinated marketing plan
- Network in relaxed, congenial settings
- Gain insight into key trends and customer plans
- Enjoy complete peace of mind

SPONSORSHIP OPPORTUNITIES

- Presenting Sponsor
- Platinum Sponsor
- Gold Sponsor
- Speaking Opportunities
- Exhibition Booth
- Technology Showcase
- Lanyard Partner
- Technology Focused Roundtables
- Entertainment Sponsorship
- Technology Networking Lunch/Dinners and more..

FOR SPONSORSHIP & EXHIBITION BOOTH
Prabhas Jha (Sales) – +91 9899707440, prabhas.jha@expressindia.com, **Srikanth RP** (Editorial) – +91 9819687097, srikanth.rp@expressinidia.com
FOR SPONSORSHIP & EXHIBITION BOOTH
New Delhi: **Prabhas Jha** - +91 9899707440, prabhas.jha@expressindia.com | **Mumbai**: **Ravindranath Nair** - +91 9820955602, ravindranath.nair@expressindia.com
Ranabir Das - +919820097606, Email:ranabir.das@expressinida.com | **Bangalore / Chennai / Hyderabad**: **Durgaprasad Talithaya** - +91 9900566513, durga.prasad@expressindia.com
Kolkata: **Debnarayan Dutta** - +91 9051150480, debnarayan.dutta@expressindia.com, **Ajanta Sengupta** - +91 9831182580, ajanta.sengupta@expressindia.com
FOR DELEGATE REGISTRATIONS : **Vinita Hassija** - +91 9820590053, vinita.hassija@expressindia.com

EXPRESS COMPUTER

Vol 29. No. 12. DECEMBER, 2018

Chairman of the Board
Viveck Goenka
Sr. Vice President - BPD
Neil Viegas
Asst. Vice President - BPD
Harit Mohanty

Editor
Srikanth RP*
Sr. Associate Editor
Sudipta Dev
Assistant Editor
Nivedan Prakash

Delhi
Mohd Ujaley, Sandhya Michu
Mumbai
Abhishek Raval, Mohit Rathod, Salvi Mittal
Bengaluru
Rachana Jha

DESIGN
Asst. Art Director
Pravin Temble
Chief Designer
Prasad Tate
Senior Graphic Designer
Rekha Bisht
Graphic Designer
Gauri Deorukhkar
Layout
Vinayak Mestry

Photo Editor
Sandeep Patil

DIGITALTEAM
Head of Internet
Viraj Mehta

MARKETING
Prabhas Jha
Durgaprasad Talithaya
Debnarayan Dutta
Ravindranath Nair
Ajanta Sengupta
Aparna Tawade

Circulation
Mohan Varadkar

Scheduling
Santosh Lokare

PRODUCTION
General Manager
B R Tipnis
Manager
Bhadresh Valia

IMPORTANT

Whilst care is taken prior to acceptance of advertising copy, it is not possible to verify its contents. The Indian Express (P) Ltd. cannot be held responsible for such contents, nor for any loss or damages incurred as a result of transactions with companies, associations or individuals advertising in its newspapers or publications. We therefore recommend that readers make necessary inquiries before sending any monies or entering into any agreements with advertisers or otherwise acting on an advertisement in any manner whatsoever.

Express Computer®
Regd.No.REGD.NO.MCS/066/
2018-20. RNI Regn.No.49926/90.

Printed and Published by Vaidehi Thakar on behalf of The Indian Express (P) Limited and Printed at Indigo Press (India) Pvt.Ltd., Plot No.1C/716, Off. Dadoji Konddeo Cross Road, Byculla (East), Mumbai 400027 and Published at 1st floor, Express Towers, Nariman Point, Mumbai 400021.
Editor: Srikanth RP *
* Responsible for selection of news under the PRB Act. (Editorial & Administrative Offices: Express Towers, 1st floor, Nariman Point, Mumbai 400021)

Copyright © 2017. The Indian Express (P) Ltd. All rights reserved throughout the world. Reproduction in any manner, electronic or otherwise, in whole or in part, without prior written permission is prohibited.

Srikanth RP, Editor
srikanth.rp@expressindia.com

The continued rise of third party cyber risks

A recent report by security firm, Gemalto, revealed that 3.24 million records were stolen or exposed in 2017 – a statistic that has increased by a huge 783 per cent over the last year. The report points out that the main cyber security risk comes from malicious outsiders who were responsible for 52 per cent of all breach incidents. In an increasingly digital world, as more applications are accessed across a diverse network of private and public clouds by external users, the risks posed due to access given to third parties is huge.

> To prevent attacks due to unauthorised third party access, it is important to hold all contractors and vendors to the same security standards

Globally, a significant number of breaches have been traced to third parties. In July 2018, a security researcher found out tons of sensitive documents from leading automakers on the open Internet. The breach was traced to one small Canadian company called Level One Robotics and Controls. The firm specialised in automation process and assembly for OEMs and Tier 1 automotive suppliers. The leak exposed sensitive information such as factory floor plan and layouts, invoices and contracts. The companies that were affected due to this leak were reputed names such as Ford, Toyota and GM. This example is not an isolated one. Retail giant, Target, which suffered financial damages of close to US$ 1 billion because of a massive data breach, had its attack originate from its HVAC vendor. Similar was the case with Equifax.

A survey by Ponemon Institute corroborates this fact. It states that 56 per cent of organisations have had a breach that was caused by one of their vendors. In another survey by Soha Systems' Third Party Advisory Group, 63 per cent of all attacks were traced directly or indirectly to third parties. This research also highlighted why third party breaches continue to be a major source of data breaches. Many CISOs believe that providing third party access is complex and has too many moving parts. For example, the survey notes that the IT function has to touch close to 14 network and application hardware and software components to provide third party access.

To prevent attacks due to unauthorised third party access, it is important to hold all contractors and vendors to the same security standards. It is also important to regularly conduct audits of the systems of the vendors to find out if the third party has in place the required policies, security infrastructure and employee training to ensure security of your data. It is always said that the weakest security link is the human element, and this risk assumes a different dimension, when it comes to third parties.

MORE INSIDE

COVER STORY

SPECIAL FOCUS: ENTERPRISE SECURITY

INTERVIEW

FEATURE

EVENT

MUMBAI
Ravi Nair/Aparna Tawade
The Indian Express (P) Ltd.
Business Publication Division
1st Floor, Express Tower,
Nariman Point, Mumbai- 400 021
Board line: 022- 67440000 Ext. 527

Aparna Tawade
Mobile: +919870853253
Email: aparna.tawade@expressindia.com

Ravi Nair
Mobile No. +91 9820955602,
Email: ravindranath.nair@expressindia.com

Branch Offices
NEW DELHI
Prabhas Jha
The Indian Express (P) Ltd.
Business Publication Division,
Express Buliding,
B-1/B Sector 10, Noida 201 301,
Dist. Gautam Budh Nagar (U.P.) India.
Board No : 0120 6651 500, Ext:270
Direct No : 0120 665 1270
Fax No : 0120 4367 933

Prabhas Jha
Mobile : +91 9899707440
Email id: prabhas.jha@expressindia.com

CHENNAI
Durgaprasad Talithaya
The Indian Express (P) Ltd.
Business Publication Division,
8th Floor, East Wing,
Sreyas Chamiers Towers
New No.37/26 (Old No.23 & 24/26)
Chamiers Road,
Teynampet, Chennai - 600 018

Durgaprasad Talithaya
Mobile: +91 9900566513
Email: durga.prasad@expressindia.com

BENGALURU
Durgaprasad Talithaya
The Indian Express (P) Ltd.
Business Publication Division
502, 5th Floor, Devatha Plaza,
Residency road, Bengaluru- 560025

Durgaprasad Talithaya
Mobile: +91 9900566513
Email: durga.prasad@expressindia.com

HYDERABAD
Durgaprasad Talithaya
The Indian Express (P) Ltd.
Business Publication Division
6-3-885/7/B, Ground Floor,
VV Mansion, Somaji Guda,
Hyderabad – 500 082

Durgaprasad Talithaya
Mobile: +91 9900566513
Email: durga.prasad@expressindia.com

KOLKATA
Debnarayan Dutta,
Ajanta Sengupta
The Indian Express (P) Ltd.
Business Publication Division,
JL No. 29 & 30, NH-6,
Mouza- Prasastha & Ankurhati,
Vill & PO- Ankurhati, P.S.- Domjur
(Nr. Ankurhati Check Bus Stop),
Dist. Howrah- 711 409

Debnarayan Dutta
Mobile No. +91 9051150480,
Email: debnarayan.dutta@expressindia.com

Ajanta Sengupta
Mobile: +91 9831182580
Email : ajanta.sengupta@expressindia.com

AHMEDABAD
Nirav Mistry
The Indian Express (P) Ltd.
3rd Floor,
Sambhav House,
Near Judges Bunglows,
Bodakdev,
Ahmedabad - 380 015,
Mobile No. +91 8866874517
Email: nirav.mistry@expressindia.com

SBI STEPS UP DIGITAL ACCELERATION WITH YONO

In its bid to become one of the top 10 digital banks in the world by 2020, SBI is banking heavily on this single, unified platform which is being used for end-to-end customer acquisition

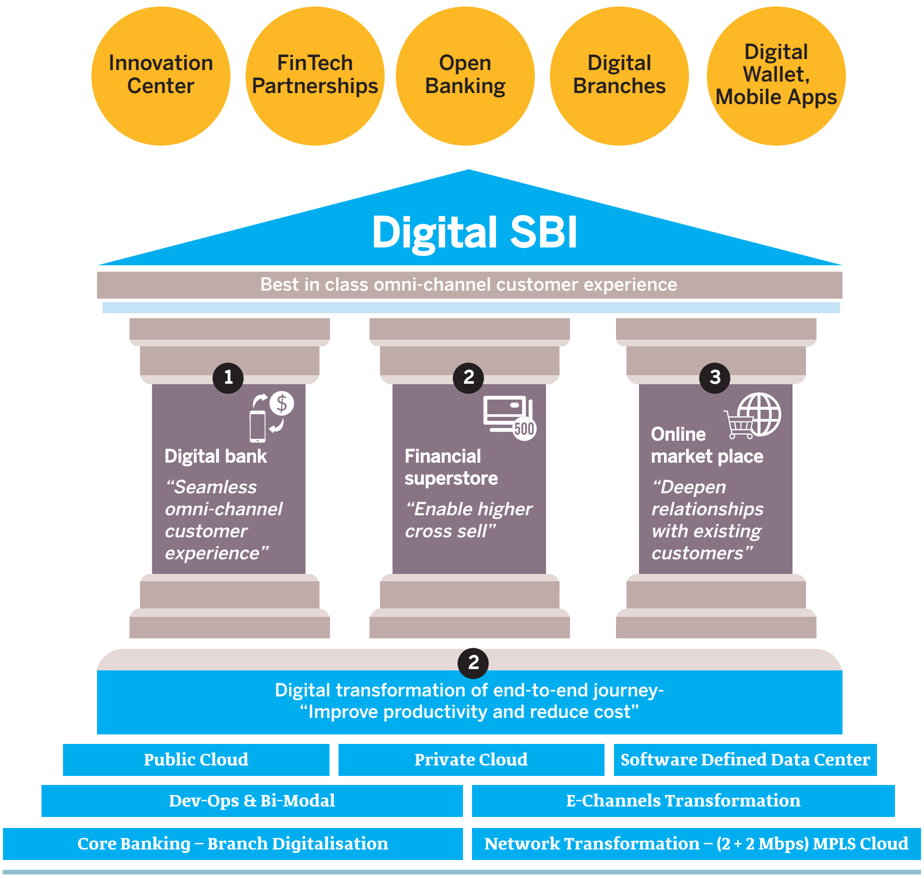
Nivedan Prakash
nivedan.prakash@expressindia.com

The use of technology to radically improve the performance or reach of enterprises has been a hot topic for every CIO. Today, enterprises across industries are using digital advances such as analytics, mobility, social media, IoT, robotics, blockchain, machine learning, advanced communications and collaboration, and are trying to bring remarkable improvement in customer experience, time to market, internal processes, and other value propositions.

BFSI is one such industry vertical that continues to drive innovation with the help of technology. In this era of self-service, organisations in this sector are trying to automate every process where technology can improve efficiency with minimal human intervention. Having said this, successful digital transformation comes not from implementing new technologies but from transforming the organisation to take advantage of the possibilities that new technologies bring to the table.

State Bank of India, the country's leading public sector bank, is the classic example of simplifying the digital experience. As SBI wants to be one of the top ten digital banks in the world by 2020, every initiative taken by the bank has its roots in a digital strategy.

SBI'S DIGITAL JOURNEY


Innovation Center
FinTech Partnerships
Open Banking
Digital Branches
Digital Wallet, Mobile Apps
Digital SBI
Best in class omni-channel customer experience
1
Digital bank
"Seamless omni-channel customer experience"
2
500
Financial superstore
"Enable higher cross sell"
3
Online market place
"Deepen relationships with existing customers"
2
Digital transformation of end-to-end journey- "Improve productivity and reduce cost"
Public Cloud
Private Cloud
Software Defined Data Center
Dev-Ops & Bi-Modal
E-Channels Transformation
Core Banking – Branch Digitalisation
Network Transformation – (2 + 2 Mbps) MPLS Cloud

Shiv Kumar Bhasin, CTO of SBI, says, "Today, banks have to make huge technology investments to enhance customer experience. Rather than the customers approaching us, we should be more proactive in reaching out to customers to understand their financial needs. In such scenario, you can function like or be called a true digital bank."

Project YONO

State Bank of India has undertaken a slew of key initiatives to drive tangible business results. The bank's most large-scale, well-planned digital transformation initiatives are centred on re-visioning customer experience, operational processes, and business models. The usage of digital technologies has helped in enhancing customer experience, streamlining operations, and creating new revenue streams for the bank.

In this endeavour, the bank launched SBI YONO (You Only Need One) about a year back, which is an integrated digital banking platform that aims to be a one stop solution for banking, lifestyle, insurance, investment, and shopping needs of the customers. There are a number of things that can be done through this app, including applying for loans, opening a savings account instantly or even shopping online. YONO is available on both Android and iOS platforms.

Many of SBI's and its subsidiary financial products offerings such as SBI Cards, SBI Caps, SBI Mutual Funds, SBI General and SBI Life, has been integrated into the YONO app. Users of the app can also apply for loans, such a home loans and auto loans. Apart from this YONO is being used for fund transfers and even to get a loan/overdraft against Fixed Deposit.

Bhasin states, "We have launched SBI YONO across the country with the aim to offer next-generation banking services to India's growing mobile phone and tech-savvy customer base. This platform not only provides unique digital experience to its customers but also makes various lifestyle, entertainment, journey and other shopping requirements available in one app through more than 85 e-commerce merchants across 19 categories."

He further points out, "It is a single, unified platform to access SBI Group's services. The key pre-requisite for this platform was to have an omni-channel and omni-device having an event-driven architecture, wherein we have used advanced analytics based not only on any customer's past transaction behaviour but also looking at the current customer profile or his spending pattern. This is the kind of intelligence we have built which was earlier missing in our internet or mobile banking platform. We wanted to build a true digital bank and with this approach, we will surely become one of the top 10 digital banks in the world."

The bank is witnessing a good traction over YONO, particularly the younger generation customer which enthuses SBI to come up with such offerings. There are already more than 10 million customers on board YONO and the bank is adding about 31000 new customers on this platform per day. And surprisingly, about 80 per cent of these new customers are in the age bracket of 22-30, which is in line with the bank's focus to target millennials.

"By March 2019, we want at least 15 million customers to come on board at our YONO platform. And by 2020, we want about 25 per cent of the bank's revenue to come from the digital bank i.e. YONO platform.," adds Bhasin.

"At SBI, we are also referring digital banking as 'empathetic banking' where we empathise with the customer's life events like birthdays, anniversaries, retirements, promotions, purchase categories he/she falls into, average monthly balance, average weekly ATM withdrawal, etc. We are capturing these moments and monitoring these behaviours and then give them curated offers or improve the financial product offerings. While we are acquiring these customers in the real-time, the end-to-end process is being done with the help RPA (Robotic Process Automation)," explains Bhasin.

The bank is also launching YONO Cash, wherein the customers do not require to carry debit card to withdraw cash from any SBI ATM. In the YONO app, they just need to key in the amount and set up the PIN for the transaction. After reaching the ATM, they need to enter the amount, their mobile number, and the earlier PIN set for the transaction. The customer will receive another PIN from the system and upon keying the new PIN, the money will be dispensed from the ATM machine. This is totally a card-less transaction.

"We are also planning to work with very large wearable devices vendors where we can have alternate, contact-less payments. Even for cheque processing, we have put up RPA agents. For example, when cheques are scanned and data processing is done, the cropping of data from the cheque and sending it to settlement houses – these all are done by RPA agents. Besides, we are also releasing APIs for fintech firms. In the YONO platform, we have set up our own bot, which has been developed in-house using advanced AI, analytics, ML, and NLP," highlights Bhasin.

Other digital initiatives

Another digital initiative is targeted at the branches, wherein the aim is to digitise all the branch processes under the 'Rupantar' initiative. It also at the core digitises the branch processes associated with CBS. The initiative will lead to reducing queues at branches. The employees are also being trained for this, for which a separate platform in the form of a multi-lingual bot has been formed, which is called 'Rupantar Genie'.

The bank is also moving towards an approach of having end-to-end banking platforms that are completely digital. "This is done using micro services, API layer. It should not be a monolithic platform but scalable and services oriented. KYC, compliance, account system, pricing – all can be done taking these technologies approach. To achieve this objective, the bank is building an innovation center. The fintech companies will be co-located onsite to collaborate with the bank to work on-premise. The bank has so far worked with more than 150 startups on various cutting-edge technologies including chatbot and data analytics," asserts Bhasin.

SBI is also tapping its employees towards making them 'intrapreneurs' and funding them to create solutions. The theme is to build the bank as a technology platform that is producing technology powered products and services. The IT strategy is targeted not only to enhance customer experience, but also to transform the workplace. The bank had the fastest Office 365 implementations in 90 days. The teams are using collaborative technologies like Kaizala app, and Skype, which is used more compared to face-to-face meetings.

The other initiatives include devising a threat perception dashboard, working on a customer communications platform, and an alternate biometric system for differently abled employees. A state-of-the-art command centre is also operational that will monitor the CBS and all the customer channels. It will also monitor the state of each of the ATMs of the bank. Furthermore, the bank is moving the branch servers on the cloud. With this, they can be accessed on a BYOD model and across omni-channel.

From the blockchain perspective, the bank has set up remittance corridor based on blockchain between SBI India and SBI Nepal. In fact, SBI is one of the first banks in Asia to go live with blockchain based remittance.

Driving future growth

To drive the future growth, SBI is working on server-less architectures. Looking at the size of the bank, wherein it has 450 million customers and 750 million accounts, it is going for container-driven architecture, where it can have scalable design.

After the Supreme Court's decision on Aadhaar based authentication, from the security perspective, SBI is putting a huge emphasis on and looking at bringing automation for other documents like passport, driving license, and PAN card among others. Here, the bank is putting AI and ML-based authentication wherein the authenticity of these documents could be determined by the robot. "If a customer comes into a branch for physical document verification, the teller already has the information from the robot whether the documents are authentic or not," asserts Bhasin.

Again, from the security standpoint, the bank has enhanced its perimeter or edge-level security using AI, ML, and robotic process vigilance. Here, the robots are going to monitor the user behaviour of the applications.

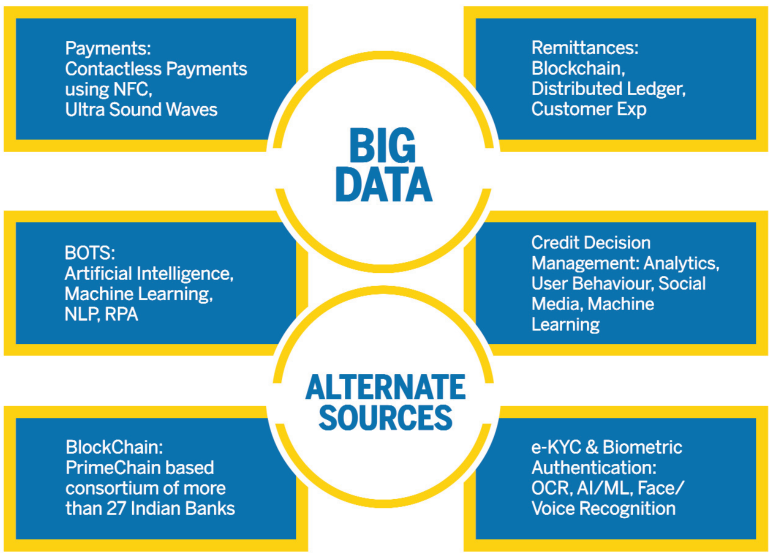
He further points out, "The bank is also working on an 'Adaptive Security Framework'. Since it is an omni-device, omni-channel bank, the customer might have logged in from his home PC or an iPad. Here, the bank should be able to detect whether it is mobile app, iPad app, or a desktop app, as the customer might have logged in from different devices. To find out the authenticity of the customer, we will not only send an OTP but also do facial recognition. And with regards to facial recognition, we will capture and detect the liveliness of the face in a unique manner so that somebody does not play static photo or video to get into the app. Additionally, we are working on speech recognition piece as well, which is again being developed in-house."

The bank has also set up a 1000 racks fully software-defined data centre in Hyderabad and it is quite bullish on implementing its private cloud, as this is going to be the largest in the BFSI industry. Here, SBI will carry out the complete end-to-end auto provisioning for the bare metal and systems software as well as application software and from there, it will deploy technologies based on container-driven architecture.

Furthermore, in order to bring better ROI of its network architecture, the bank is setting up SDWAN and is planning to do POC with 500 branches. This is one strategic network transformation program. To improve the branch network, the bank is working with various players like BSNL to bring our key branches in cities on to the fibre.

"From the lending perspective, we will have a fully digital lending on the YONO platform for the car and home loans, wherein the in-principle offer will be given to the customer instantly on the mobile device and we will be carrying out not only the credit bureau checks but also various other checks which enrich the decision management by the underwriter. Robo advisory and personal finance are the other areas that we are going to work on the YONO platform," concludes Bhasin.

Current FinTech engagements with SBI


Payments: Contactless Payments using NFC, Ultra Sound Waves
Remittances: Blockchain, Distributed Ledger, Customer Exp
BIG DATA
BOTS: Artificial Intelligence, Machine Learning, NLP, RPA
Credit Decision Management: Analytics, User Behaviour, Social Media, Machine Learning
ALTERNATE SOURCES
BlockChain: PrimeChain based consortium of more than 27 Indian Banks
e-KYC & Biometric Authentication: OCR, AI/ML, Face/ Voice Recognition

Security is foundational and a key enabler for digitisation

RAMCHANDRA HEGDE, Vice President, Global Information Security, and IT Compliance, Genpact explains how the CISO's role is multi-dimensional and the type of risks they face

By Rachana Jha

What are the challenges faced by CISOs on the InfoSec front?

While the specifics will vary by industry and company, the CISO's role is multi-dimensional, having aspects spanning strategy, operations and execution, risk management and regulatory compliance. CISOs have to understand an organisation's business objectives and imperatives, its risk appetite and threat and regulatory landscape, and accordingly build and run a program, which involves influencing and orchestrating a number of moving parts across the enterprise – all in an environment of rapidly evolving threats, technological changes and ever increasing digitisation. Additionally, having core internal security capabilities is a requirement for most organisations, and in the current situation with demand far outstripping supply, getting and keeping the right talent is a big challenge.

On one hand when the wave of digitisation is shaping the future of businesses, it's also bringing along the challenge to robustly secure the very critical customer facing and the native IT infrastructure. How do you see this challenge?

Security is foundational and is a key enabler for digitisation and helping organisations build digital trust with their customers. First, core hygiene practices e.g. vulnerability management, identity and access management are critical and are baseline measures. Second, security controls specific to cloud hosting (configuration management and visibility), and digital asset security (dynamic and static testing) need to be in place. Finally, newer concepts relevant to cloud and digitisation (containers, DevOps, IoT) need to be understood and appropriate security controls designed and integrated.

Please share some best practices to be followed to maintain a robust IT security posture

There is no silver bullet. While the latest advanced technologies and tools get a lot of attention and are required in some cases, there is no shortcut to following the basic principles and getting core hygiene in place across the key pillars of security - people, process, technologies, and partnerships. Also, while there is a lot of focus on acquiring security technologies, deploying them optimally and utilising their capabilities well is essential to realising the benefits. Security is also a risk management function, and it's imperative to have the lens of risk and weave that into security processes.

> Integrating security into processes and creating a security culture are all other critical aspects which must be addressed to get security right, so aside from funding, the management needs to ensure there is broader overall support and sponsorship

How important is awareness as a good number of breaches happen due to the insiders not following the security hygiene practices?

Again, a foundational element of security is people. There is also a distinction between being aware and a true behaviour or culture change – e.g. one might be aware of good practices yet not follow it if it is too difficult or they have not fully internalised the risk. Thus organisations should look beyond just awareness as in broadcasting good practices. Good design of systems and security controls and usage of "nudges" (concepts from behavioural economics) are examples of how an organisation can be more effective in this area.

What is your view on IT budgets? Are CISOs getting enough?

With the increasing broader awareness of the threat environment, impact of breaches and destructive attacks, and penalties under laws and regulations, I would think most organisations would understand the criticality of information security and support it with appropriate funding. Getting funding is only one dimension though, if, for example the technologies procured are not adequately utilised, the desired outcomes will not be met. Also, integrating security into processes and creating a security culture are all other critical aspects which must be addressed to get security right, so aside from funding, management needs to ensure there is broader overall support and sponsorship for the program.

Do CISOs have a say in board meetings?

Given its criticality to businesses, information security is definitely an area for Board oversight, and while the specifics of which Committee(s), topics covered, frequency, etc., will vary by organisation, the CISO has an important role in ensuring the Board is apprised of the company's infosec posture and addressing questions they have.

Ensuring powerful and multi-layered safeguards

TO COMPLY WITH GDPR, VFS Global has implemented a 13-point privacy framework that enables the company to operationalise the requirements of the GDPR, and measure compliance with it. **Barry Cook**, Privacy and Group Data Protection Officer, VFS Global, gives the details

Salvi Mittal
salvi.mittal@expressindia.com

A data protection officer is an independent governance role that manages a company's compliance with existing data protection laws of the land in which the company operates. It is not part of the operational teams and has a reporting line directly to the highest level of management. Barry Cook is Privacy and Group Data Protection Officer at VFS Global, who is accountable for ensuring that the company handles the personal data of visa applicants and its employees in a manner that is compliant with the law and also with the company's own internal data protection policies, to ensure that the privacy of this data is maintained at all times during its life-cycle.

Data privacy overview

As a company, VFS Global operates across over 140 countries and handles large volumes of applicant information (for visas and citizen services). The company is one of just 35 per cent of global companies that are GDPR-compliant (as per a Talend report published in September 2018). This means that they are complying with demanding standards set by the various aspects of the European data protection regulation, which came into effect in May 2018. Similarly, they are compliant with data protection regulations of all countries they serve and operate in.

Modern data protection laws seek to find a good balance between the rights of the individual and the interests of organisations who process that data. Putting personal data processing in a robust and workable data protection and privacy framework is a high priority at VFS Global. "We have in place a complex, robust and multi-layered safeguards at the digital (server infrastructure) and physical (at our Visa Application Centres or VACs) levels so that the high standards set by GDPR forms the global baseline for data protection," says Cook.

In order to be updated, they also monitor the development of data protection laws in the countries that they operate. This way the company can be proactive to ensure that it stays compliant to new laws as well ensuring that the processes are effective and don't result in increased administrative burden at the VAC level.

Even before GDPR, the company has always had strong information security practices in place, with robust frameworks for handling data and an existing compliance-driven culture, as per the strict requirements laid down by client governments. "To comply with GDPR, we have implemented a 13-point privacy framework that enables us to operationalise the requirements of the GDPR, and measure compliance with it," he adds. Cook further explains by giving an example, "We put in place various processes for receiving consent from applicants for storage of their personal data, online and offline. Extensive training of our staff has also been part of our preparations. Many companies are looking at GDPR compliance as a means to strengthen their data and privacy norms, and naturally so, since this new era of data regulations heralds a data revolution."

In the last few years, the conversations around data protection and data privacy have underscored a better understanding of the core philosophy of management of personal data. It is important to remember that organisations simply 'borrow' an individual's personal data for the purposes of performing a task. No more than that specific task.

"The best-case scenario for allowing flexible transfer of data, while also ensuring the security of personal data, is based on the standard of 'adequacy of transfer'. This means one country or organisation must determine that another country or organisation has sufficient data protection safeguards to ensure that the rights and freedoms of individuals travel with their data. Once the country or organisation is satisfied that the destination country has adequate safeguards in place, data can be transferred easily. Clearly, this must be underpinned by the capability of national data protection agencies to be able to perform checks of compliance and to be able to take corrective or punitive action if required," mentions Cook.

Mitigating security challenges

As the world's largest visa service provider that handles sensitive information of millions of applicants in more than 140 countries, for 61 client governments, it has always been incumbent on VFS to put rigorous data security checks in place. "As such, in terms of technical and organisation measures for data security, we were already at an advanced level even before the GDPR – having attained ISO 27001 certification for Information Security Management Systems, our IT teams were well aligned with operating with strict controls. We also utilise sophisticated cyber security and threat detection tools as the nature of our business demands this," he reveals.

An important aspect of data privacy controls is ensuring employees across the global operations are adequately sensitised to the context and necessity of the protocols. So the company had to initiate a global internal awareness campaign to explain the basics of data privacy concepts to employees and this greatly facilitated the adoption of the data protection processes and procedures that followed. Large organisations who are attempting this for the first time may find this a challenging task, but it is an essential one, believes Cook.

> As the world's largest visa service provider that handles sensitive information of millions of applicants in more than 140 countries, for 61 client governments, it has always been incumbent on VFS to put rigorous data security checks in place. In terms of technical and organisation measures for data security, we were already at an advanced level even before the GDPR

Strategic approach

Data breaches are an expected risk to any organisation that is processing personal data. Therefore, it is vital to have in place both technical and organisational measures that detect, mitigate and recover from data breach, such that the risk to the personal data involved is minimised. "At VFS Global, we use some very sophisticated detection tools that alert the security team of a potential incident. However, technology can only go so far and we recognise the value of the human element when it comes to data breach prevention. We encourage our employees to be very vigilant about risks which might manifest themselves at any time," he states.

Impact of AI

Artificial Intelligence (AI) is the latest trend in data processing and as such has the potential to greatly change the way in which visa processing is performed. "That said, we have to look at just how AI based process will take decisions. One of the fundamental tenets of AI is that the algorithm 'learns' from each decision made. A classic example of this is VFS Global's first digital employee ViVA, the first-ever chatbot in the visa services space. ViVA offers applicants round-the-clock support for visa queries, akin to any highly trained customer support executive. In effect, AI has to go to school to learn how to make decisions that are fair as well ethically and morally correct. This is where the privacy professional has to ensure that privacy by design is built in from the very start," he explains.

'We have a well-defined information security governance framework'

IN AN EXCLUSIVE interaction **V Swaminathan**, Head - Corp Audit & Assurance, Godrej Industries, discusses the security framework in the group, and highlights how India's first Data Protection Law will be impacting them

By Salvi Mittal

Please provide the information security overview at Godrej Industries

At Godrej Industries, we believe that information security can be achieved as a result of collective efforts between business, IT and the information security team. Support from the top management is crucial when it comes to establishing an effective information security framework. At Godrej Group, we have a well-defined information security governance framework with definite roles and responsibilities across each business unit. The stakeholders work in co-ordination with each other to implement the information security policies effectively. Transparency in the systems is maintained by presenting the updates on the current happenings to the management committees on a periodic basis.

How is Godrej Industries embracing digital security?

We understand the requirement for digital transformation for business visibility and productivity, by providing ease of computing and flexibility to our employees. However, the fact is digital transformation in any organisation undeniably opens up a new set of cyber risks and threats. In order to encounter the expanding cyber surface, we have devised a simple two-pronged approach. Firstly, we bring in the information security perspective and controls right at the design phase of any digital transformation initiative. Secondly, we believe in continual improvement of security measures which are adaptable and scalable as per the changing technology landscape.

Please provide some recent examples of innovations/ projects driven by you

In lieu of the constant technological advancements, we believe in continual improvement of our security framework. We keep on evaluating various tools and technologies for cyber threat hunting in order to build a proactive security framework. In the manufacturing setup, we think that IoT is the next big thing. It is a comparatively new technology, which is being tried and tested in parts. We have been looking into development of security framework for IoT, which will be integrated with our overall security framework.

How do you fit security within your corporate culture?

While an organisation can have all the advanced tools and monitoring mechanisms in place, information security initiatives can be effective only when the people recognise and acknowledge their responsibility towards it. We try to implement measures so as to create an all-inclusive information security organisation. We have a defined code of conduct, which is signed off by employees at the time of on boarding. We conduct regular awareness sessions across all locations on the changes in the information security landscape, its impact on organisations and how as employees we can be mindful of these risks. The group keep the employees updated by sending notifications on the current cyber security threats through our internal social media platforms. Also, there is a mechanism in place enabling employees to reach out to the information security team with subject matter experts and report their concerns or seek guidance as required.

What are the possible challenges in your industry and how are you mitigating the same?

In the manufacturing industry, information security is not highly regulated as opposed to that in the financial and banking industry. Accordingly, a lot of effort has to be invested in convincing the business for implementation of any new security initiative. To tackle this we periodically present updates on information security threat landscape and the corresponding solutions, which are followed by constructive discussions pertaining to value delivered by the solutions post which such initiatives are taken up for implementation. Also, in the manufacturing industry, implementation of information security controls at a factory setup is challenging. The workforce at the factory setup is more of operational in nature and so there is an inherent gap in the requisite information security skill set. To bridge this gap, we conduct periodic information security trainings at the factory sites and also conduct assessments to verify the design and effectiveness of these controls.

How will the new data protection law affect you?

At Godrej Industries, we give high importance to customer data privacy and the upcoming data protection laws will help us instill the same in our culture. With the introduction of general data protection regulation 'GDPR' we initiated the discussions and comprehensive assessments of our data protection framework. We perceived this as not just a compliance requirement but as best practice and accordingly we implemented these controls not only for our European customers but for Indian customers as well. So by the time Indian data protection bill was introduced we already had some of these internal controls implemented.

The new data protection laws are customer oriented and have a lot of specific requirements. These requirements might trigger changes in customer front-ending processes. We consider compliance to these laws important and as a group we might even consider partnering with external experts to ensure the complete compliance.

CISOs should think strategically and align business priorities with security

IN THE LIGHT of the changing technology landscape, it's very important for CISOs to adopt a particular security framework. This will instill a basic information security discipline among the various stakeholders in the enterprise environment, feels **Uday Deshpande**, Group CISO, Larsen and Toubro

Abhishek Raval
abhishek.raval@expressindia.com

The barrage of evolutionary concepts like blockchain, AI, etc are enhancing the efficiency and productivity of the organisation. As a parallel, these digitisation initiatives are also bringing along challenges on the security front.

It's becoming challenging for CISOs to protect the content that is getting exposed online, because of a multitude of data streams getting generated due to digitisation. Most organisations are moving towards a perimeterless environment, which is blurring the boundaries between the company's internal and external environment. The data'- both structured and unstructured, is getting exposed online. The Information Security (InfoSec) professionals are finding it increasingly challenging to secure this information in absence of effective discovery and classification machinery. The regulatory environment is also active and the data protection law, which has many similarities with the GDPR will also make it challenging in terms of identifying the personal data and then giving the adequate protection layers to the specific information such as employee and customer sensitive data.

At this juncture, when there is a shadow IT environment, because of the increasing scope of interconnectivity between different digital platforms, it is becoming difficult to get the visibility of the data - where does it reside, in what format and who is the custodian.

The adversaries are also becoming very sophisticated. "The last year belonged to ransomware. This year, many instances of hacking computer systems for coin mining have been reported. Coin mining doesn't cease the company operations but hampers overall productivity," says Uday Deshpande, Group CISO, Larsen and Toubro.

So what is becoming important for CISOs ? Agility to detect and respond to these incidents. The key is reduce Mean time to detect (MTTD) and mean time to respond (MTTR) to the best extent possible so as to reduce impacts of the incident.

Importance of a base level security framework

In the light of the changing technology landscape, it's very important for CISOs to adopt a particular security framework like NIST, SCIPC, ISD, Information Security Forum, ISO 27001, etc. This will instill a basic information security discipline among the various stakeholders in the enterprise environment. The discipline should be measured and maintained on a sustained basis. Some of the important domains of information security - end user, network, software, internet, should have stringent controls and organisations as a part of the security framework should have mechanisms to measure the effectiveness of the controls put in place. The need is also to improve upon the existent practices on a regular basis.

"The most important aspect is not to have these practices being conducted as a routine task, for the sake of compliance and just to tick mark the doables, but to implement, embrace and measure them in letter and spirit," says Deshpande. It's found in many organisations that inspite of having acceptable usage policies, many executives ask for exceptions. It's important to have a dedicated arrangement for such cases. The executives should be clearly communicated that the exception will be given but only with the caveat that the data flow in their device will be monitored. Unless these policies are not clearly communicated and adhered to, people will continue to make mistakes, whether advertently or inadvertently. Thus the primary role of the CISO in the organisation is to review the effective implementation of information security policies. The CISOs should measure, improve and report the findings to the management through risk governance.

Create your own framework

Deshpande also suggests CISOs to create their own framework. One size fits all frameworks might not be possible and give the desired results. "The CISOs should pick only those controls which are really applicable and fits the company's requirements. The relevant requirements from different frameworks, like NIST, ISF and ISO 27001, etc, should be collected and put together into the customised framework and implemented, in the best possible way in an automated manner, which very well fits the requirements of engineering industries," he says. The reason being, the sites of engineering industries, at times are located in far fetched areas. There is hardly any technology involved and thus to monitor them becomes challenging. In these scenarios, automation helps. Moreover, it also helps in actively measuring the different parameters of that site over longer durations and with complete accuracy. Otherwise, there are chances of the local officials fudging the data.

The key is to measure the effectiveness of the customised framework. "You can only mature what you have measured and acted for improvements," states Deshpande.

IT security budget

These frameworks ask for technology tools, which have costs involved. The CISOs might not always get the required budgets. "A few years back, the budgets were incident driven. An information security breach incident would probably help in getting budgets approved. However, over a period of time, information security has gained the mind share because of the personal breach incidents like credit card frauds, Facebook related breach incidents, email phishing, etc. There is much more acknowledgement of the potential of the damage these incidents can have on the organisations too," says Deshpande. This wasn't the case earlier. The board wasn't taking information security seriously and nobody was interested in talking about the threat.

The CISO now is getting ample support from the board. This refers not only for the IT security budget but also for getting the related manpower. The visibility of the CISO and the InfoSec department is increasing in the board and as a result, budgets are generally available with adequate reasoning. The main challenge for the CISO, is to justify the budget asked for. The best way is to measure the cost of the incident and justify the budget. The other ponderables for the CISOs include selection of technologies. There are a plethora of options available at the end user, network, periphery and at the cloud level. The key is to collaborate with the right combination of technologies, for them to work with synergy. For example, in case if there is a breach at the laptop level, the information should be shared automatically at the network level and with the required firewalls to block similar traffic.

Inculcating a culture of security

Security is 20 per cent technology and 80 per cent human. Before any new technology implementation, security has to be thought of at every stage of the process - designing, testing, production, etc. Every user in the IT chain is a key stakeholder in security.Without diluting the importance of technology tools, the human aspect to information security is crucial. Without the active and alert participation of the employees, customers, etc., organisations will keep on suffering from cyber attacks. Generally, it is found that there are many instances of requests from key employees and in some cases from senior management to have USB access, access to the social media sites and email sites which may ultimately infect the systems. Similarly, if the developer introduces a cross-site scripting or SQL injunction vulnerability because of not following a disciplined approach, it may lead to site crash or data exfiltration attack. A discipline has to be strictly followed, that the code should not go into production without testing. An end-to-end secure SDLC has to be followed and practiced. It's important to mention that security is always top driven and the senior management should act as role models.

(The views expressed in the article are personal and should not be considered representing the views of the company)

BSE goes live with deception technology

SHIV KUMAR PANDEY, CISO, BSE shares about Smokescreen's deception technology, which creates a layer of decoys across the entire network. When hackers attack, they unknowingly engage decoy systems that lead them into a virtual reality while raising an alarm. Deception technology makes the network exponentially more difficult for attackers to predict, understand and attack

Abhishek Raval
abhishek.raval@expressindia.com

BSE, Asia's oldest stock exchange and now the world's fastest stock exchange with the speed of 6 microseconds is a critical part of India's national infrastructure. BSE's market capitalisation has exceeded US$ 2 trillion. The stock exchange also comes under the direct monitoring of the National Critical Information Infrastructure Protection Centre (NCIIPC). Being in such a position makes BSE a prime target for cyber-attacks, not just from financially motivated hackers but also nation states.

"We have a 360-degree approach to protection at BSE. The way we think about cybersecurity is not just in terms of prevention but also detection and response. Prevention technologies are necessary, but attackers find some way or the other to breach perimeter defenses. As a result, we've made threat detection and response an integral part of our security stack. Deception technology is one of the most advanced threat detection approaches in the market right now," says Shiv Kumar Pandey, CISO, BSE. It doesn't rely on static signatures or heuristics. Being attack vector agnostic, it is highly accurate and provides broad threat coverage with low false positives. It is easy to deploy and has no performance impact.

Smokescreen's deception technology creates a layer of decoys across the entire network. When hackers attack, they unknowingly engage decoy systems that lead them into a virtual reality while raising an alarm. Deception technology makes the network exponentially more difficult for attackers to predict, understand and attack.

Deception technology from Smokescreen meets three key objectives:

- **High network visibility** - Smokescreen's approach to decoy deployment covers the entire network. Credential decoys detect attempted privilege escalation at the endpoint level, threat intelligence decoys identify internet originating attacks, and file decoys protect high-value target personnel who might be attacked as part of a campaign to obtain their access right or information.
- **Low false positives** - Smokescreen's deception platform has a low false-positive property by design. Decoys are deployed strategically across servers, the user network, and DMZ. No legitimate user is supposed to open a decoy file, log-in to a decoy application or use decoy credentials. So when Smokescreen raises an alert, the security team is able to drop everything and investigate it with confidence.

> Smokescreen's deception platform has a low false-positive property by design. Decoys are deployed strategically. No legitimate user is supposed to open a decoy file, log-in to a decoy application or use decoy credentials

- **No performance impact** - At BSE, the median trade time is 6 microseconds making us the fastest stock exchange in the world. Therefore, performance is a crucial consideration when we evaluate solutions. Smokescreen was the only deception solution that met this criterion. Smokescreen decoys are deployed without any agents. They are passive detectors that don't generate any latency like perimeter technologies. At the endpoint level, the decoys are non-invasive. Finally, Smokescreen doesn't slow down the network because it does not generate network traffic or require bandwidth.

The technology went live in Sep 2017. "Smokescreen is already helping us overcome several challenges. The solution provides full kill-chain coverage. It can detect pre-attack reconnaissance, spear-phishing attacks, privilege escalation, lateral movement, and attempted data-theft. Crucially, Smokescreen is easily scalable. Their Threat-Parse technology generates full attack reconstructions in natural language making it easy for our security team to analyse an attack and act. In summary, Smokescreen has brought down our mean time to detect, know, and respond significantly," says Pandey.

It integrates with SIEM. Events in the SIEM are enriched with attack logs, Indicator of Compromises (IoCs), and threat intel feed. As such, the exchange observes a lot of activity on various traps, but the ones which are investigated are based upon the magnitude, the type of attack observed, IP reputation, etc. All this activity has been observed in real-time.

The information gathered from investigating activities from these traps is provided both for strategic and tactical insights. This information has also been shared with regulators and organisations like CERT-In. "They have appreciated such inputs and post their investigation it has been observed that same signatures were identified in other big corporations," shares Pandey.

How a CISO can play it smart

JAGMOHAN SINGH, CISO, Canara Bank describes how digital transformation is happening at a rapid pace and the various ways for CISOs to smartly navigate through the many tough challenges

Rachana Jha
rachana.jha@expressindia.com

CISOs today are required to smartly formulate policies and undertake information security vision, duly keeping in mind the infosec strategy as per industry risk perspective, global risks at that point of time, business strategy as well as the regulators' perspective, while tracking the balance between risk optimisation, business realisation and resource utilisation. "Though the challenges are many, I would like to discuss a few top pain points which disturbs every CISO in the current environment. Firstly , most of the intelligence feeds comes in the form of bad IPs, hashes or url, the same are not sufficient and are very deceptive. Hackers are seen to adopt various techniques to manipulate and bypass such feeds and being able to dig deep into the organisations' network. Over and above, in case of file-less attacks or In-Memory execution of malicious code/scripts along with legitimate or whitelisted processes, there is a need to consider some different approach which can provide proactive intelligence for timely detection and quick remediation. Thus, I feel that there is a need to fill this gap by a more matured approach which proactively sense the threats well in advance on the basis of industry specific IOCs (Indicators of Compromise) and actions required as responses," says Jagmohan Singh, CISO, Canara Bank, adding that this approach should focus on identifying the TTPs (Tactics or tools , Technique and Procedures) adopted by hackers/fraudsters preparing a directory/ knowledge base of IOCs. TTPs and patterns identified in respective security domains like server, endpoints, network, application and databases, etc., should be mapped to IOCs, which in turn should be plugged to actions for incident response and the same needs to be automated (fully or assisted) with clear categorisation into discretionary and mandatory actions.

The second biggest challenge is to establish a connect between SOC teams and Red teams. SOC teams need to holistically consider the results of penetration testing or red teaming for improvisation of IOCs/use cases. However, there is a disconnect between the two, which is the major cause of cropping up of weaker controls and subsequent compromises, as is seen across the industries. "I feel there should be a purple team concept be made mandatory for better exchange of information and well defined collaboration between the two teams in the interest of matured monitoring, early detection and quick reactions," states Singh.

The third challenge, which according to Singh, is having high impact, is the lack of skilled cyber security professionals. It is difficult to find the right talent for security monitoring activity, incident response activity and for proactive detection tasks like ethical hacking, red teaming etc. Apart from this, there is a positive increase in attrition rate being recorded for core cyber security functions.

With the advent of newer delivery channels and collaborations, the business dealings and transactions are becoming more and more complex and volatile. The fundamental approach in such a scenario is to practice 'Open But Secure'. Since, businesses are collaborating and partnering, a lot of data exchange is taking place across entities using various techniques like Web Service, APIs, infra sharing, etc. "This brings into the picture various new threat vectors for data integrity, data secrecy and privacy compliance related issues. My advice to security practitioners is that while following the basic pillars of information security, we must also concentrate on defining a thorough and well-designed strategy for collection of security intelligence and correlation in order to achieve initiation of pre-emptive actions for probable threats. Of course, security awareness would also be playing a critical role in efficient detection and aversion of cyberthreats," states Singh.

Robust IT security

"Apart from following the best practices, correlation of intelligent information from different sources within organisation as well a external/commercial intelligence feeds plays a very crucial role in deriving a robust security posture for any organisation. In fact, apart from preventive controls, detection and response is the 'mantra' in current times. However, certain best practices of utmost importance includes; keeping the security patches updated, following a defined SOP for updation of patches whether its OEM or SI (temporary patches) , when patches are received through mail or remote method a system to ensure its authenticity including approval to apply (using checksum etc) to be ensured," he informs. Further, benchmark configuration documents and automated logging and alerting on the departure from approved configuration is also important. Since, for most of the threat vectors, phishing (or its different flavours) is emerging as prominent attack vector and as such user awareness about such tactics and methods becomes very important. Apart from the aforesaid practices, another basic practice is to conduct a periodic and holistic review of network architecture and firewall rules.

Awareness is going to play an important and deciding role in days to come. "We should understand that hackers follow the principal of least resistance. As such, instead of trying time consuming attack vectors, perpetrators are more than happy to use our people for executing what they want. In one of the recent attacks, the payload was dropped into the system in form of a phishing mail containing patch for one of the system, which was installed by the administrator due to lack of control over Patch Management process. Thus, the spending on creating awareness and trainings on security issues and best practices in infra, coding and development, etc., be considered as a major strategic investment."

Replying to the question on if the CISOs are getting enough for IT budgets, he says, "I feel this depends on the support of the senior management and the culture within the organisation. The organisation, which are matured and well sensitised, towards cyber environment, their boards are considering cyber security as a major business enabler and in turn they are tuned to release a balanced budget for critical security projects. However, there are organisations which are not able to foresee cyber as a risk, again due to lack of matured Risk Management approach, do not provide due budgets to CISO teams and becomes susceptible to hackers' community. In fact, the budget for security should be based on a well-defined business risk assessment carried out for identification and prioritisation of business assets under cyber threats."

> Instead of trying time consuming attack vectors, hackers are more than happy to use our people for executing what they want

Trends in digitisation business

While various technologies are making an impact on the way organisations function, Singh feels there are few technologies which may see larger penetration and amalgamation with digitisation of businesses. "AI is the one which has already started making its way in productivity. AI just does not mean RPA or intelligence replacing human effort, but with AI for the future, I mean to say augumented intelligence assisting humans in creating user interface, automated decision based intelligent triggering of actions and analytics. Further , we can see greater merger of AI and IoT technologies as IoT use is increasing in all spheres," he remarks, adding that another technology where innovation is moving ahead is blockchain products.

The major hurdle in blockchain is the incentive for compute required for a project where different stakeholders have varying level of interests, however this technology is catching a significant interest of businesses to leverage performance and efficiencies.

The ecosystem has to come together to protect each other

IN CASE AN incident happens in one part of the system, the partners should be willing to share the same with the entire ecosystem. This process needs to happen seamlessly, says **Ashutosh Jain**, CISO, Axis Bank

Abhishek Raval
abhishek.raval@expressindia.com

As the banks are becoming digitally evolved, it dovetails into organisations getting more interconnected with each other as a result, data, IP, transactions, etc., gets shared using technology tools. In such a scenario, banks have to adopt a wholesome security approach to safeguard the interest of the customers. It not only requires securing the organisation's IT infrastructure but also that of the entire ecosystem.

What has changed, after the wave of digitisation that is spreading fast, is the new threats, which didn't exist before. The API web getting created around institutions needs breach protection as the digital supply chain players are highly connected. A malware infection in one part of the system can have a contagion effect across the board; data leakage in one institution can affect its partners and also customers to an extent.

There are technical solutions available to neutralise these deficiencies. But the fundamental issue is not with selecting the technologies, but the mindset. "Some supply chain players may be hesitant in sharing any security related information updates, which may be due to various reasons, however, information sharing and collaboration is the key. In case an incident happens in one part of the system, the partners should be willing to share the same with the entire ecosystem. This process needs to happen seamlessl," says Ashutosh Jain, CISO, Axis Bank.

Communicating with the board: Keep it simple

The Board understands the need for strengthening the security system at all levels. The need for strengthening the IT security has never been an issue. "The Board understands the requirements. CISO's prioritisation and what delivery matters the most. Generally the boards of all financial institutions are concerned about the readiness of their respective companies. Board members are curious about the time frame required to plug any cyber security gaps, as are general breaches are made known in media or otherwise. In such cases, it is better to avoid communicating the technical complexities and keeping it simple for Board and top management briefings," states Jain.

"The plethora of emerging technologies are now so advanced that the real challenge lies in understanding and dealing with the complexity of the emerging technologies and the risks germinating from them," adds Jain.

Changing role of CISO

The CISOs should continue to remain technically focused and keep up to the speed with the organisation's business topology. Some of the skillsets, that will be in demand in the security industry include security operations, threat modeling, data scientists, who have the knack to extract or decipher the threats which are low and slow, etc. Generally security professionals should choose to specialise in one of the three mindsets, i.e. risk, security or audit mindset.

> What has changed, after the wave of digitisation, is the new threats. A malware infection in one part of the system can have a contagion effect across the board; data leakage in one institution can affect its partners and also customers to an extent

Whenever any organisation suffers security incident, big or small, the leadership and technical preparedness always get tested. The emergence and evolution of new technologies, especially public cloud, community open source, etc., also brings along with them the challenge of speedy and sound investigations, in case of a breach incident. Lack of well-rounded understanding of these technologies may be big impediment for security professional in-charge of such investigations.

The CISO is also responsible for continuous monitoring in organisations. The CISOs should move the needle from basic risk approach to an advanced threat discovery mindset, to look for specific opportunities of data leakage, malware infection to save the reputation damage.

Different organisations have different teams for conducting audits, which should work hand in hand with IT and CISO to ensure alignment of priorities and hence results.

Ethical hacking as a means for discovery of general controls weakness will continue to be used by CISOs. It's generally being conducted across the financial industry and has proved effective over the years. It has been successful in highlighting the vulnerabilities, which remain undetected in the regular testing cycles. However, the practice should be done with caution.

India is emerging to be a promising country for security startups. DSCI has played a major role in introducing them to the corporates. Indian startups are doing well in the area of malware detection, honeypots and deception technology, security analytics.

'Information security is a journey and not a destination'

IN AN INTERACTION Satyanandan Atyam, Vice President, CRO, Max Bupa Health Insurance, describes the challenges faced by CISOs, how they are mitigating the same and what are the best practices to be followed to maintain a robust IT security

Rachana Jha
rachana.jha@expressindia.com

Challenges faced by CISOs are manifold. To champion the information security agenda in the business organisation, the CISO should be able to bring the future into the present so that he can do something about it now. This ability to provide the visibility of a future prepared organisation to business is critical. "The capability to bring the bottom up risk assessment on the technology controls, which could help to gauge if the organisation is future ready, and convincing the management is needed. The CISOs do not get the mandate to make the organisation future ready. They struggle to get the organisation operate with security controls as per the risk assessment of existing risks. The challenge around budgets approvals for information security initiatives is a pertinent issue because RoI's for such investments cannot be arrived. Though there have been attempts to create models around the RoI calculation, there has always been a challenge to convince the CFO organisation,"says Satyanandan Atyam, Vice President, CRO, Max Bupa Health Insurance.Digital, real time analytics and AI adoption would be differentiators for the business to acquire and engage the customer. To implement these business requirements, require the IT to re architect/punch holes into the facades of security infra around the IT infrastructure. "This augments the risk surface for the organisations and they need to design and implement security technologies which are secured and enable an open IT architecture. The juxtaposition of the need and the risk is like a double-edged sword for the technology and risk teams," he mentions.

Best practices

Atyam believes that information security is a journey and not a destination. There are always new challenges to meet. Executing a security strategic plan is a critical success factor for organisations that truly want to maximise their ability to manage information risk. Committing to this process takes resources and time. The best practice/baseline practices for the organisation to maintain a robust security posture are as below:

- Identify your crown jewels
- Prioritise the data which needs to be protected
- Determine risk appetite basis risk assessment
- Implement IT controls basis the risk assessment
- Have review and response processes and strategies
- Assess the maturity of the cyber security framework-testing methods

These should be part of the information security strategy of the organisation. A strong defense can't happen if what is being defended isn't understood. "The process should also determine how each asset impacts your operations and may include financial implications, reputational damage, or loss of business opportunities. This will help in prioritisation of efforts. Firms need to be aware of what policies and procedures they currently have in place including what solutions and controls can be added by their IT vendor to enhance their security. Be aware of what safeguards are available to assist you with your existing programs. Risk assessment would help in understanding the cyber security risks to the firm's operations, functions, image, reputation, and assets," avers Atyam.

Insider risk

The breach anatomy will increasingly trend towards either by the errors committed by the insiders or by the malicious insider initiating a connection to the external world. A malicious connection created from a trusted source (inside the organisation) to malicious outsider is always effortless. This change in the attack methods has made it increasingly important to have awareness for the insiders and critical to plug the backdoors of any IT footprint for exploits. "The IT organisations are not control savvy and the vulnerability are left open for exploits. This poor hygiene in the internal IT environments is a risk which needs to be attended, not through an audit mechanism but through IT function driving the security as an agenda," points out Atyam.

The CISO's budget still piggybacks on the IT budgets. They still are not being provided separate budgets under the ambit of the risk function. This would continue till the point the share of information security initiatives is for the implementation of the IT security controls is higher.

Nowadays CISOs are being invited to the Board meeting to provide an assurance on the information security posture of the organisation. The relevance of information security is being a critical differentiator for business to contain risk and to ensure their digital journey is secured. CISOs would not have a say in decision-making at the Board, but are being heard when they table the risk and applicable risk containment initiatives.

> The breach anatomy will increasingly trend towards either by the errors committed by the insiders or by the malicious insider initiating a connection to the external world

Array Networks reiterates its commitment to the Indian market

IN AN EXCLUSIVE interaction with CRN India, **Shibu Paul**, Regional Sales Director – APAC, Array Networks, highlights the company's business strategies in India, its contribution to the hyper convergence market, and the focus on long-term relationship with customers. Some edited excerpts...

By Nivedan Prakash

What is your perception of Array Networks' business growth in India, when the market is undergoing a lot change and witnessing a slowdown?

We are growing at a positive rate of 35 per cent YOY. 2018 has been a rewarding year for Array and we should exceed our revenue numbers. The colossal growth is backed by the significant deals in BFSI, Government and enterprises. We have invested heavily in all the verticals.

Besides, our newly launched hyper converged networking and security platform solution, AVX, has received great reception from channel partners as well as customers. Recently, we even had a large enterprise deployment for our hyper converged network infrastructure solution. Also, our selected channel partners have been trained well to take Array's hyper converged infrastructure solution into the market.

How is the market for hyper convergence evolving? What has been your contribution to address new customer requirements?

We can't deny the fact that hyper convergence is taking over the market at a high pace. Companies are increasingly embracing hyper converged infrastructure as a go-to technology platform to address security, productivity and other concerns. It not only delivers the performance companies are looking for, but also brings other benefits, including less networking, storage or physical equipment. It lowers IT costs, accelerates speed to market and reduces complexity related to the IT environment and the business as a whole.

Working on the same lines, we developed AVX Series Network Functions Platforms. Array's AVX Series Network Functions Platforms address the challenges of both VARs and MSPs through hyperconverged platforms that offer the agility of virtual appliances with the performance of dedicated appliances. Each platform supports multiple instances of Array or third-party networking and security functions. VARs can develop new best-of-breed security and networking packages to differentiate their offerings while consolidating multiple discreet appliances into just one or two rack units; end-customers benefit from reduced rack space, power, cooling and cabling requirements.

We are committed to the Indian market and have lined up investments to support and serve our customers efficiently with high breed solutions. Having said, we are all set to inaugurate Array innovation labs in Bangalore with a world class testing lab for third party networking and security functions by December 2018.

Where are you planning to set up these innovation labs?

We will have our central innovation laboratory in Bangalore following extended lab setups in other metro cities, namely, Mumbai and Delhi. These innovation labs will primarily focus on building products in the security, analytics and reporting space, which is the current requirement of end customers.

We have the budgets approved and we have been looking to hire the right skilled talent who can help us in making this journey productive. We are basically looking at candidates with engineering knowledge, who have worked with end customers and large OEMs in the past. The key objective is to have a core team focusing on local and global customer requirements. There is a huge potential in the market and we want to be well equipped and armed to address the various opportunities.

What are your views regarding the increasing global investments made in the Indian market. Where do you see the opportunities?

Array acknowledges that India is one of the fastest growing economies in the world and continues to propel in the coming years.

Today, the Indian market is on the target list of a lot of organisations who are looking to invest. Being in the market for so long, we understand the dynamics and have already started investing heavily in security and infrastructure solutions. To stay ahead in the game we have planned to have a development hub in India to cater for future products to the global and local markets.

Array Networks has a very stable customer base. What are the factors that have contributed in this strong customer loyalty over the years?

Array Networks has crossed more than 300 enterprise customers in India. One of our core strengths has been dedicated local support ecosystem. The support team has been increasing with the increasing customer count. We have a regional support system to address the issues across India.

> We are committed to the Indian market and have lined up investments to support and serve our customers efficiently with high breed solutions

Besides, Array was one of the first and few vendors to setup local RMA and local support infrastructure. Now we will be investing in local development teams to bring global innovative solutions to Indian customers. We have been able to manage the implementation timeline, in the given time frame which has favoured us a lot.

Most of our customers have been with us for a long time and we believe that our alliances will continue to grow in the future as well. Array's customer retention has been one of the highest in our segment and adds one more feather to our cap.

What have been your channel expansion and investment plans?

We have a dedicated channel ecosystem. With support of our channel partners, we are focused on developing a skilled pool of resources. We have various channel schemes that have been recognised and well accepted by our partners. Schemes include assured margin program, assured incentive programs for leads, PoC's to name a few. Our objective has been to ensure that channel partners are rewarded for every effort and not just for sales. There is a concentrated effort to enhance training activities for channel partners to develop and certify them.

We are looking to add more partners for our hyper convergence business. We are creating an infrastructure today for tomorrow.

Since you provide dedicated hardware and infrastructure for your customers, do you have any plans to spin this as a service model through your partners?

Our strategy is to offer services through the leading CSPs in the country. We are already working with CSPs like Netmagic to provide services through them. We will help the CSPs to create an infrastructure which could offer our services at attractive price points. Besides, we will introduce a service model specifically for government customers as per the guidelines along with CSPs.

What kind of qualities do you look for while partnering with channel partners? Are you looking to expand your network?

We have more than 60 channel partners currently. Since our solutions include NFV and hyper convergence in networking and security, we look at the partner's knowledge in networking, virtualisation and security. These three things need to fall in place.

In the near future, we will add large SI's with a good skill sets in virtualisation, security and networking to train them on our AVX platform. Array supports SI's who want to put up a lab for array commercially and technically. We have few partners who have already invested in setting up the labs for Array. In addition, channel partners who are already selling HCI solutions from Nutanix make a good fit as we are complementing each other.

Apart from the Government and BFSI, which are the other verticals you would want to focus on?

Apart from the Government and BFSI, enterprise has been our focus area. With our AVX network and security virtualised platform, we expect to make great inroads into the large and medium enterprise customers. 2018 has seen a phenomenal contribution from the enterprise customers with AVX. Another segment we see potential is the service providers. From SI perspective, we would want to partner with SI's who are addressing the global markets.

Feature

How an AI startup is partnering with police to solve high risk cases

GURGAON BASED STARTUP, Staqu, is using AI technology to solve hundreds of tough cases, including breaking terrorist modules in Punjab

Sudipta Dev
sudipta.dev@expressindia.com

When Staqu was established in 2015, its founders, tech enthusiasts Atul Rai, Anurag Saini, Chetan Rexwal, Pankaj Sharma had the vision of plugging in AI and deep learning solutions into daily life. Based out of Gurgaon, Staqu began its journey through developing advanced neural networks and hybrid models to tackle persistent issues in the Homeland Security domain. The company is currently active with three products at the state-level, namely ABHED (Artificial Intelligence Based Human Efface Detection in Rajasthan), PAIS (Punjab Artificial Intelligence System in Punjab) and PAIS (Police Artificial Intelligence System in Uttarakhand). "Additionally, we have also integrated our AI software with smart glasses for the assistance of police forces. It helps in identifying a person in real-time with credentials. This is particularly useful in analysis of crowd and traffic," says Atul Rai, Co-Founder & CEO, Staqu.

Explaining how the solutions have helped the police departments in the states of Punjab, Uttarakhand and Rajasthan, Rai states, "Our customised solutions converted the chunks of physical data available with the police and intelligence agencies into substantial information to power the decision-making through real-time metrics. We currently have over six lakhs criminal records in all forms – image, text and voice that has helped police forces to solve over 400 high risk and complicated cases."

Highlighting the successful initiatives with the Punjab police, which brought a great sense of accomplishment to the company, Rai mentions, "The entire project was administered under the leadership of Mr Nilabh Kishore, IG/ IPS of the Organised Crime Control Unit in Punjab. Within the early days of deployment, we had helped the police department solve nearly 200 high risk cases, breaking the terrorist modules."

Tech-enabled assistance to police

Rai and his team are now gearing up for a pan-India expansion, partnering with different police departments and ushering them in the era of real-time, tech-enabled assistance. "With the advent of Smart Cities in India, we would also be engaged in devising ways to make predictive policing a reality in India," affirms Rai.

Predictive policing

Staqu's predictive policing solution has also effectively helped Dubai Police. Rai reveals that Dubai Police is aiming for a 25 per cent reduction in violent crimes by 2021. It is further intent on integrating artificial intelligence with its current programs and databases, to provide analytics and statistics that would support the decision-making process, hence enabling quicker response time in emergent situations. "We cannot tamper with the confidentiality status, but every region of the world has a vast difference in terms of societal issues and AI builds the common ground to address them. Staqu is amongst the four startups that were finally selected to work with Dubai Police on their varied set of challenges out of the 677 global applications," he says, pointing out that on the technical front, the company's successful pilots of heterogeneous model for crime detection and prevention in real-time with the domestic agencies, makes it stand apart, internationally.

The company is focused on research and innovation to bring cutting-edge solutions for police departments and reduce the crime rate. "We have been working on utilising AI and machine learning for deeper analysis," mentions Rai, adding that for instance, they focus on "gait" analyses to recognise miscreants by the manner of their walking. They are also concentrating on speech biometrics and the innovative violence recognition and crowd analysis to provide next-level quick assistance to homeland security personnel.

With time and expertise, Staqu discovered the potential in the e-commerce and smartphone industry with products such as 'VGREP' and 'Minus Infinity' respectively. "With our one of its kind offering and capabilities in addressing the heterogeneous data, in terms of speech, text and image, Staqu could utilise its AI algorithms to elevate its credentials in the research domain. As of 2018, we have more than 25 published research papers in world renowned journals and conferences. Most recent was the increment in accuracy by 9 per cent (89.5 per cent on VoxCeleb data set) in the field of speaker identification," says Rai.

> We currently have over six lakhs criminal records in all forms – image, text and voice that has helped police forces to solve over 400 high risk and complicated cases
>
> **Atul Rai,**
> Co-Founder & CEO, Staqu

Some of the major milestones for Staqu include accreditation and acknowledgement by IBM in its GEP Smart Camp for two consecutive years, a win at the 'Tech Rocketship Awards' conducted by the British High Commission, in the NASSCOM 'League of 10' and win as a 'AI Game Changer' in the year of 2018. The vision of Staqu's leaders is to empower and enable the country to perceive the future with AI.

CX is key for business growth

EXPRESS COMPUTER MAGAZINE in partnership with Avaya organised a roundtable in Delhi, on the various facets of customer experience

Mohd Ujaley
mohd.ujaley@expressindia.com

The Chinese proverb "A man without a smiling face must not open a shop" has an embedded message on the importance of customer experience (CX) and its impact on business. And, in today's steady rise of the customer-centric environment, it has become more relevant as brands are compelled to deliver the best CX across different platforms or point of sale. To support enterprises to offer better customer experiences, companies like Avaya have come out with a suite of cloud based solutions. Recently, Express Computer magazine in partnership with Avaya organised a roundtable discussion in Delhi on the various facets of CX for Indian businesses.

Participating in the roundtable discussion, Raj Khemani, IT Lead, Indian Sub Continent, GlaxoSmithKline said that for him the customers and consumers are different. He said that for his organisation, customer is the retail outlet because his organisation sell to them, but it is actually the consumption that drives the sales. Khemani breaks consumer experience and customer experience in two different categories. He said, "A customer needs to be serviced and a consumer needs to have a good experience." He informed that his organisation has good plans to take care of both customer experience and customer services.

On the question of one area that needs to be improved, he said that from consumer experience perspective, companies need to move beyond social media engagements. Companies should focus on innovative ways to connect and once connected, they should look at the ways to convert the engagement into real purchase.

Agreeing with the views of Khemani, Anand Ruhela, Head - IT, Kwality, said that there are three key aspects of an engagement with customers. He breaks these three aspects into before engagement, on engagement and after engagement. Highlighting these he said, "Before a customer engages with us, we need to provide them all information. This could be done by digital marketing. Second, we need to provide different method to engage with us. It could be anything from a mobile application to a phone call. Third, once they are engaged, it is really important to meet customer requirement and deadline." One of the key challenge to CX, he said, "Nobody likes delay, so it should be avoided."

Sharing his views on CX, Om Prakash Singh, Assistant Vice President - Corporate (IT), JTEKT, whose company deals with B2B business in automobile industry said all customers are OEMs and his company does not drive marketing as it is done by customers themselves. "Despite that our main work is to align with them, as we are second layer of the chain," said Singh, adding that if demand goes from X unit to Y, they need to be in align to meet it.

Singh said that one of the biggest challenges is if demand is going from X to Y – how to scale and help the customers. In addition, he explained that 10 years ago the lit time to launch a car was 3-4 years, but now within a 6-8 months, the company has a new version and the launch has some innovation so within this short time, you have to make those innovation. As the supplier how you do that – "this is the challenge," he said.

On the question of the keys of customer delight, he said that today certain things are guaranteed in a customer's mind; like quality and on-time delivery. So capturing the latent requirements of the customer and coming out with some solution and offering for him that can really improve customer experience and take the business to a different level.

Participating in the discussion, Mayank Bhargava, VP& CIO, DHFL Pramerica Life Insurance was of the view that insurance is a segment where least amount of technology has gone. He said that it is an untapped market. "There a lot of need and potential for technology intervention. Typically, the insurance industry follows the banking industry, so whatever the banking industry experienced five year ago, now we are experiencing it," said Bhargava adding that the rate of change has accelerated, so in the next few years there is going to be lot of new innovations in the insurance space.

On technology that can dominate, he said, "IoT is likely to improve the risk assessment, leading to passing of benefit to the customers, also it could be used as a tool for customer engagement."

Bhargava asserted that currently the insurance industry is very dry – "You buy a policy and absolutely there is no reason why you would engage with the insurance company until and unless you need to settle the claim. But companies are now trying means for increasing meaningful engagement with customer.

"Which is where technology can play an important role. Mobility with IoT can overhaul the engagement process," he added.

Agreeing with Bhargava, Amit Saini, Head - IT, Columbia Asia said that patients are also demanding quick report. He informed that few months ago his organisation launched a website and mobile application for providing details to the customer. "They are able to use those applications for checking reports, booking appointments and for other engagement," he said.

Kuntal Shah, Director - Sales Engineering India & SAARC, Avaya said, "In the past, there were many point solutions. But what have changed is that customers wants to come to businesses from any of the channel be it online, email, chat or phone – so, you have to provide equally good experiences on the all channels. Second, company collects tons of data. They should use those data to improve their services and customer experiences. Today's technology like AI or machine learning can help them do that."

Customer-centric organisations look at AI, ML and bots to enhance client experience

AVAYA AND EXPRESS COMPUTER jointly organised The Think Tank Forum in Mumbai, wherein digital leaders and decision makers of today deliberated closely on emerging technologies like AI, chatbots and more

Mohit Rathod
mohit.rathod@indianexpress.com

Focused on using these technologies in the existing business to create a customer-centric culture within the organisation, the roundtable event by Avaya and Express Computer in Mumbai was participated by renowned digital leaders from across industries; including Byju Joseph, CTO, Future Generali Life; Mukesh Sachdev, Head - IT, HDFC ERGO General Insurance; Vinai Krishnan Nair, Head - IT Delivery & Insurance Business Solutions, SBI General Insurance; Lalit Popli, Head - IT, ICICI Prudential Asset Management Company; Hiren Shah, CIO, Reliance General Insurance; Suresh Shanmugum, Head - Digital Innovation & Future Technology Business Information & Technology Solutions, Mahindra & Mahindra Financial Services; Bhavesh Lakhani, SVP & Head - IT, SBI Mutual Fund. In a close and informal setting, these stakeholders indulged in an insightful discussion with Team Avaya, over dinner.

Titled, "Think Tank: For the Leaders of Tomorrow", the event encapsulated various critical digital strategies such as effortless engagements with customers using social media, chat and messaging channels in a consistent manner. Furthermore, the roundtable discussion served as a platform to learn to leverage and take advantage of emerging technologies like AI and chatbots, by applying the existing business rules, and based on the context analysis of interactions; how to champion omni-channel customer experience and personalise customer interactions; create a customer-centric culture throughout an organisation and much more.

Sharing his views on how customers have become central to digital strategies or enterprises, Shah said, "Today's customers are always developing, requiring organisations to constantly refresh their focus on customer experiences. Technology plays a critical role to address this; however, digital tools have limitations in some areas. For instance, chatbots are still evolving and machine learning is still a buzzword."

In an era of instant consumption, digital services and products are raising the bar in enhancing customer experience. This is becoming more important in an era where the customer connects with the organisation through multiple touch points – mobile applications, voice, social media, messaging applications, chat, etc. To deliver a consistent engaging customer experience, organisations need solutions that transform multi-channel customer service into a single transparent omni-channel service.

To maintain a consistent brand experience, and create loyal engaged customers, it is imperative to create personalised customer experiences at every touchpoint. Sharing more, Joseph commented, "In today's world, every organisation is trying to reach out to customers through digital channels, but there are certain shortcomings in the way. Seamless experience for customers is the key and digital has to address that. Amidst the widespread talks on technologies such as machine learning, there's a need for machines to be fine-tuned to efficiently interact with customers."

The BFSI sector has been among the biggest adopters of AI-based chatbots and machine learning. Sharing the implementation aspect of these technologies, Nair said, "Chatbot and machine learning is sold at a rapid pace, but implementation is a gradual process. While enterprises are in a hurry to implement these technologies, it is crucial to understand it's a long process which requires huge data to train ML solutions," adding that even in terms of data, there are large differences according to various regions in the country.

While acknowledging the growing customer acceptance, a key shortcoming of enterprise chatbots is that they are domain-specific. This drastically limits their ability to efficiently service customers' requests when they face questions they haven't been trained to answer. Team Avaya spoke about an interesting industry-first development – a social platform for chatbots, which is aimed at taking a giant leap in customer self-service. Drawing parallels from traditional social media, Avaya's innovation provides a structured platform for bots to interact securely, aiming to extend each chatbot's expertise.

Echoeing Nair's views, Sachdev said that training chatbots is important to ensure seamless and efficient customer experience. He added, "Everything shouldn't be looked at just from an RoI perspective. We must implement technologies and evaluate results to mark the success." Whereas, Popli highligted customer acquisition, customer fulfilment and customer experiences as crucial factors. He expressed, "Customer services is one area where technology adoption is still underway."

Sharing insights on use of analytics in the insurance industry, Shah said that his organisation has not yet moved to real-time analytics; however, processes have significantly improved over time. He further added that even the government sector has identifed the potential of analytics.

REGD.NO.MCS/066/2018-20, PUBLISHED ON 28TH OF EVERY PERVIOUS MONTH & POSTED AT MUMBAI PATRIKA CHANNEL
SORTING OFFICE, DUE DATE 29 & 30 OF EVERY PREVIOUS MONTH, REGD. WITH RNI UNDER NO. MAHENG/49926/90

sify keeping you ahead

Innovate your business with the unlimited potential of the Cloud

Transform your business today to tackle the growing needs of the future with the power of the Cloud. Sify offers integrated IT Solutions for a seamless experience. Our Cloud at Core proposition is built on over two decades of experience in transforming how 8500 businesses optimize consumer and enterprise expectations. Now, you can re-engineer your business model with Sify's Cloud services.

Cloud Build | Internet of Things | UC on Cloud | Partner Cloud Services | Sify's Application Services on Cloud

Network for Cloud | Sify Cloud Services (CI) | Industry Standard Applications on Cloud | Security Services

Agility — Flexibility — Choices

Our end-to-end ICT Solutions

Network Services ■ Data Center Services ■ Cloud & Managed Services ■ Applications Integration Services ■ Technology Integration Services

marketing@sifycorp.com I www.sifytechnologies.com I +91 8750442233