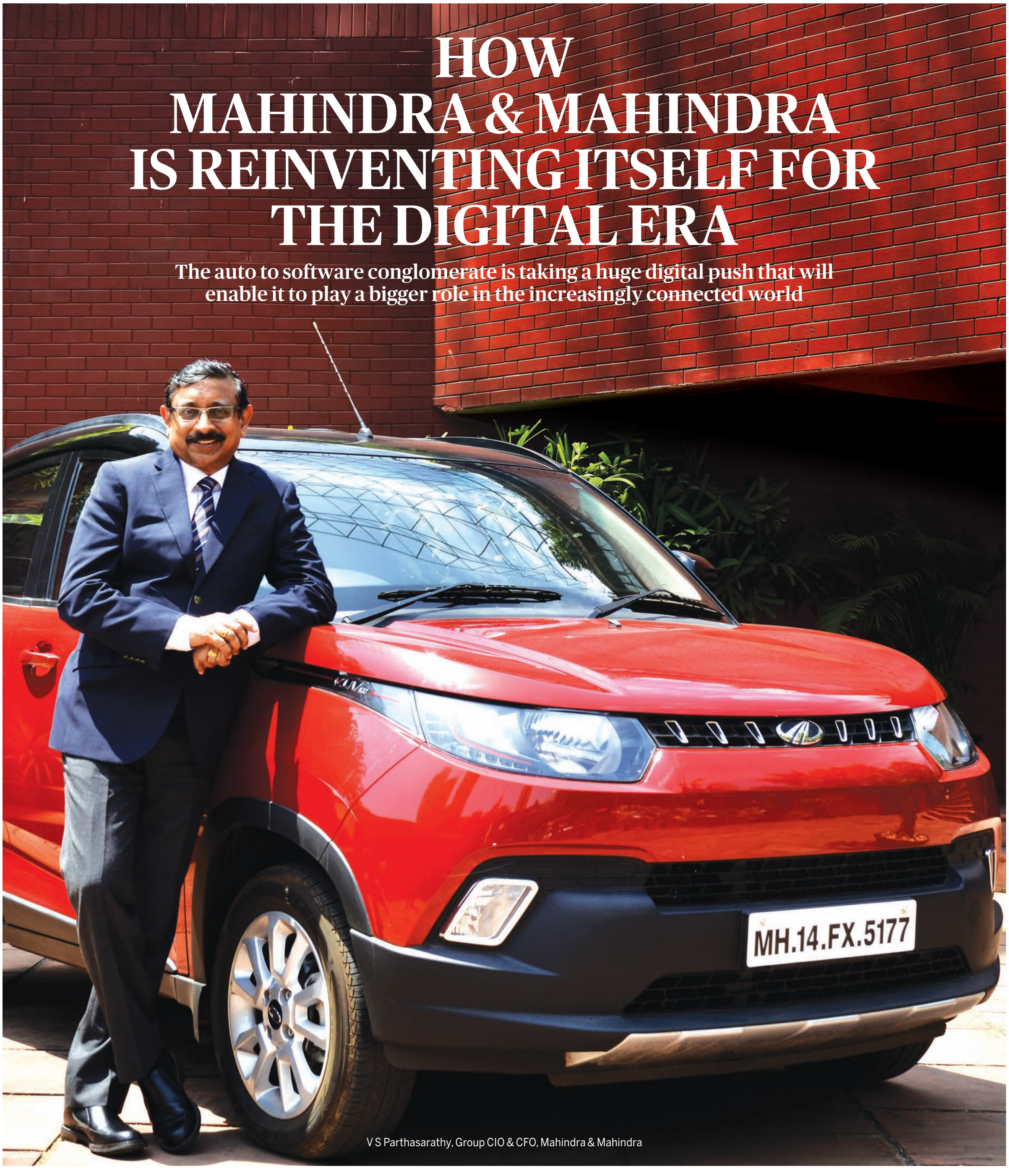
INDIA'S LEADING IT MAGAZINE WWW.COMPUTER.EXPRESSBPD.COM @ExpComputer

AN INDIAN EXPRESS GROUP PUBLICATION VOLUME NO. 29, NO.2, PAGES 16, FEBRUARY, 2018, ₹75

EXPRESS COMPUTER

HOW MAHINDRA & MAHINDRA IS REINVENTING ITSELF FOR THE DIGITAL ERA

The auto to software conglomerate is taking a huge digital push that will enable it to play a bigger role in the increasingly connected world



V S Parthasarathy, Group CIO & CFO, Mahindra & Mahindra

SOPHOS

Security made simple.

THE END OF RANSOMWARE

Everything you need to know to stop ransomware.

Know Your Enemy

Ransomware is a $1 billion dollar business that often evades traditional anti-malware.

Stop Ransomware Now

Sophos InterceptX is proven to stop ransomware in its track by blocking unauthorized encryption of files.

Stop Ransomware with Sophos Intercept X

The proven CryptoGuard capabilities in Sophos Intercept X block ransomware as soon as it starts trying to encrypt your files, returning data to its original state:

- Protects endpoints from ransomware attacks
- Automatically rolls back encrypted file changes with no loss of data
- Stops both local and remote file encryption

For more details visit www.sophos.com/ransomware

Tel: +91 79 66216838
Email: indiamarketing@sophos.com

EXPRESS COMPUTER

Vol 29. No. 2. February, 2018
Chairman of the Board
Viveck Goenka
Sr Vice President - BPD
Neil Viegas
Editor
Srikanth RP*
Delhi
Mohd Ujaley, Sandhya Michu
Mumbai
Nivedan Prakash, Abhishek Raval
Bangalore
Rachana Jha

DESIGN
National Design Editor
Bivash Barua
Asst. Art Director
Pravin Temble
Chief Designer
Prasad Tate
Senior Graphic Designer
Rekha Bisht
Layout
Vinayak Mestry

Photo Editor
Sandeep Patil

MARKETING
Regional Heads
Harit Mohanty - West
Prabhas Jha - North
Kailash Purohit - South
Debnarayan Dutta - East

Marketing Team
Shankar Adaviyar
Ajanta Sengupta
Navneet Negi

Circulation
Mohan Varadkar
Scheduling
Santosh Lokare

PRODUCTION
General Manager
B R Tipnis
Manager
Bhadresh Valia

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)

Srikanth RP, Editor
srikanth.rp@expressindia.com

Mahindra's digital leap

In the digital era, every company is facing a similar challenge: How do you compete in a world that is increasingly being dominated by born-in-the-cloud startups or digital incumbents? How do you really compete in the digital economy which has a complete different set of rules or follows no rules to compete? While some industry leaders have decided to wait till some digital technologies are proven, some like Mahindra & Mahindra look at digital as an opportunity.

> The Mahindra & Mahindra Group's digital strategy is a striking example of how Indian organizations can improve their competitiveness using digital as a strategic lever to drive growth

The group is preparing itself for a huge digital leap and relooking at how digital technologies can be used to create massive competitive advantage. For example, the group has quickly learnt from startups and digital leaders like Uber and Ola. The launch of SmartShift is a step in this direction. This is an online aggregator platform that connects cargo owners and transporters, which has become extremely popular among cargo owners due to its transparent and competitive pricing. In a first, the group has also launched an agricultural rental equipment service. Using an app, farmers can take on rent tractors and equipments on a pay-per-use basis. Orders can be booked using an app, which are then passed on to the nearest franchisee using location based mapping.

Understanding the critical importance of pro-active maintenance, the group has created, 'DiGiSENSE', a platform that connects Mahindra vehicles, tractors, trucks and construction equipment to the cloud. Using IoT, this platform enables owners, fleet operators, drivers, dealers and service teams to access vital information about their vehicles, trucks, tractors or construction equipment on a real time basis from any location. Similarly, drivers can contact emergency breakdown services or pull up a route planner at the touch of a button, fleet owners and dealers can track the location of their vehicles in real time, while remote diagnostics and reports allow service teams to monitor the vehicle's health and productivity parameters, on a real time basis.

Innovations such as the driverless tractor and using virtual reality at select dealership outlets, points out to a bold approach where the group is ready to experiment with emerging technologies. For example, the group is using IoT and machine learning technologies in one of its manufacturing plants to automate and digitize its production planning.

The digital era requires nimbleness, and the humility to adapt and accept new business models. The Mahindra & Mahindra Group's digital strategy is a striking example of how Indian organizations can improve their competitiveness using digital as a strategic lever to drive growth.

MORE INSIDE

MUMBAI
Shankar Adaviyar/Ravi Nair
The Indian Express (P) Ltd.
Business Publication Division
1st Floor, Express Tower,
Nariman Point, Mumbai- 400 021
Board line: 022- 67440000 Ext. 527
Mobile: +91 9323998881
Email: shankar.adaviyar@expressindia.com

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

Branch Offices
NEW DELHI
Prabhas Jha, Navneet Negi
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

Navneet Negi
Mobile No. +91 8800523285
Email: navneet.negi@expressindia.com

CHENNAI
Kailash Purohit
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

Kailash Purohit
Mobile No. +91 9552537922,
Email: kailash.purohit@expressindia.com

BANGALORE
Kailash Purohit
The Indian Express (P) Ltd.
Business Publication Division
502, 5th Floor,
Devatha Plaza, Residency road,
Bangalore- 560025

Kailash Purohit
Mobile No. +91 9552537922,
Email: kailash.purohit@expressindia.com

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

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

E.Mujahid
Mobile: +91 9849039936,
Fax: 040 23418675
Email: e.mujahid@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

HOW MAHINDRA & MAHINDRA IS REINVENTING ITSELF FOR THE DIGITAL ERA

The auto to software conglomerate is taking a huge digital push that will enable it to play a bigger role in the increasingly connected world

V S Parthasarathy, Group CIO & CFO, Mahindra & Mahindra

COVER STORY

Srikanth RP
srikanth.rp@expressindia.com

As a group, the Mahindra & Mahindra has always taken a series of ambitious initiatives throughout its history. For instance, it was one of the first players to start creating electric vehicles, before the concept of electric vehicles became popular. More recently, the group announced the launch of India's first driverless tractor, an innovation that can lead to improved productivity for farmers. Today, even as India looks to embrace electric vehicles in a big way in an aim to reduce dependence on import of oil, the Mahindra & Mahindra group is placed in a sweet spot.

In this age of digital disruption, the group is tinkering with emerging technologies as an early start can be a massive competitive advantage. For instance, it was one of the first conglomerates to experiment with Blockchain. The Mahindra & Mahindra Group collaborated with IBM to consider the potential of using Blockchain in supply chain finance. This was a pioneering initiative, as this was one of the first Blockchain-based supply chain finance solution in an industry other than banking.

Being a large conglomerate, the group understands the need of creating new business models using the power of technology. V S Parthasarathy, Group CIO & CFO, Mahindra & Mahindra, echoes the thoughts of his group when he says, "In this age of digital disruption, experiential commerce will change how the customer experiences commerce, which in turn, will have an impact on business models. Organizations have to think on how they can help customers experience a 'wow' factor. I want all of our industries to be the trendsetters in the digital world. My vision is that all our 21 industries will be digital world leaders in their own ways, and IT will be our partner in this."

> In this age of digital disruption, experiential commerce will change how the customer experiences commerce, which in turn, will have an impact on business models. Organizations have to think on how they can help customers experience a 'wow' factor. I want all of our industries to be the trendsetters in the digital world. My vision is that all our 21 industries will be digital world leaders in their own ways, and IT will be our partner in this
>
> **V S Parthasarathy**
> Group CIO & CFO, Mahindra & Mahindra

As a starting point, the group has already started creating a common integrated customer database of all Mahindra customers. Companies within the group function as part of federated structure, with their own strategic and decision mechanism serving their customers independently. However, this is a digital initiative to consolidate the customer data of various companies, to provide one view to the group.

Parthasarathy says that organizations need to rethink on how their business models must change. "The new world will be B2C – it will not be a world built to last, but it will be a world built to change. Your old cost structure will have no place in the new world, so you have to reset and reboot your costs. Every organization should continue to dramatically think how do we enable business, enhance it, and engender. Seventy per cent of the focus today is on enabling business and 30 per cent on enhancing and engendering, but in the new world, it should be vice versa. In order to be a value creator, organizations will have to commercialize business models of IT in terms of products and solutions, look at the customer as the king and focus on creating immersive digital experiences for them." The group has started acquiring companies that fit this vision. For example, Tech Mahindra, acquired UK-based firm, The BIO Agency, which specializes in transforming customer experience using digital services.

One of the best examples that explains the group's thinking is the SYOUV platform which has been designed to help a customer who is currently in the pre-purchase phase. It provides a collection of important information regarding a Mahindra vehicle. It also offers personalized recommendations based on the customer's actions on the platform. A feature named 'Talk to Expert' allows customers to get answers to their queries in real-time through audio/text chat. The '3D Discovery' shows various features of a Mahindra vehicle in a rich 3D format. There is also a 'Collaborative Exploration' feature on offer through which, users can invite their friends on Facebook and email to collectively customize Mahindra vehicles. More recently, to help probable customers have a better experience of its e20 Plus electric car, the group is providing virtual reality devices at select dealership outlets to highlight key features of its car.

Predictive maintenance

In the enterprise, the notion of predictive maintenance using IoT is well known. Mahindra & Mahindra has used IoT intelligently to bring in a new level of experience for vehicle owners. The group launched 'DiGiSENSE', a platform that connects Mahindra vehicles, tractors, trucks and construction equipment to the cloud, opening up a whole new dimension to the experience of vehicle ownership. This launch made the company the first OEM in India to integrate its product line-up onto a cloud-based technology platform. This platform enables owners, fleet operators, drivers, dealers and service teams to access vital information about their vehicles, trucks, tractors or construction equipment on a real time basis from any location.

"With 'DigiSense', it will be the first time in India, that we will be able to do servicing, sales and solutions – all digitally – across our portfolio," states Parthasarathy.

Similarly, drivers can contact emergency breakdown services or pull up a route planner at the touch of a button, fleet owners and dealers can track the location of their vehicles in real time, while remote diagnostics and reports allow service teams to monitor the vehicle's health and productivity parameters, on a real time basis.

Taking a cue from Uber and Ola, the group has launched an online platform, SmartShift, that connects cargo owners and transporters. The technology provided by a company incubated by Mahindra & Mahindra, aggregates demand and helps cargo owners find the right transporter or logistics provider based on specific parameters such as weight and shipment size. This has become extremely popular as transparent and competitive pricing is visible to both cargo owners and transporters. It is also possible to track and trace vehicles to ensure safety of cargo.

Tweaking the Uber model, Mahindra has launched agricultural rental equipment services. Using an app (Trinngo), farmers can take on rent tractors and equipments on a pay-per-use basis. Orders can be booked using an app, which are then passed on to the nearest franchisee using location based mapping.

Another innovative app called the 'With You Hamesha app' enables customers to check their car's service history, book a service slot and even create a job card to get an online service estimate. It also allows users to track servicing of their vehicles and establish a video connection with a relationship manager to get real time updates on the service. Customers can also opt to pay the service bill online through the app and can request the vehicle to be delivered to a specific address.

The future

The most striking aspect about Mahindra's digital transformation vision is that the group is taking an innovative approach and is willing to tweak established digital models to the market it serves. The digital world needs quick adaptation and willingness to learn from different industries. This is a world as Parthasarathy describes, 'a world built to change', and companies who consistently and quickly adapt will lead. The Mahindra & Mahindra group has shown this agility by willing to partner with startups and create innovative business models using the power of technology.

MAJOR DIGITAL INITIATIVES

- **DiGiSENSE (Connected Vehicle platform):** DiGiSENSE is a technology solution that connects Mahindra vehicles, tractors, trucks and construction equipment to the cloud, opening up a whole new dimension to the experience of vehicle ownership.Its launch has made the company the first OEM in India to integrate its product line-up onto a cloud-based technology platform.

- **Blockchain supply chain financing:** Mahindra, along with IBM, is developing a cloud based Blockchain solution for supply chain financing. This is designed to transform supplier-to-manufacturer trade finance transactions through a permissioned distributed ledger. The blockchain-based supply chain finance solution will enable all parties involved in the transaction to act on the same shared ledger, with each party updating only their part of the process, ensuring efficiency, consistency, trust and transparency, while safeguarding sensitive information

- **SmartShift:** SmartShift is a technology enabled load exchange platform. SmartShift will act as an exchange platform for cargo owners and transporters, enabling them to work with each other. Cargo owners (both businesses and individual users) can access the SmartShift service through a world class mobile app (available on Android), the website or the dedicated call centre.

- **Trringo:** Trringo is a first-of-its-kind tractor and farm equipment rental business that aims to raise the level of mechanization in Indian farming. Not every farmer can afford his own tractor. Small farmers ask for tractors from the few who own those, leading to uncertainty, compromise on quality of tractors or equipment, and often, disappointment. That's where Trringo comes into the picture.
  Now, whenever farmers need a tractor or any farm equipment, they can simply call Trringo, or use its mobile app, and place their order. They will receive a well-maintained tractor along with a professional driver with utmost ease. Not only can they get their work done in a stress-free manner, with consistent use of mechanisation, their productivity increases too.

- **With You Hamesha:** With You Hamesha platform is aimed at improving post-sales customer satisfaction levels. Through the With You Hamesha app, customers can check their car's service history, book a service slot and even create a job card to get an online service estimate. It also allows users to track servicing of their vehicles and establish a video connection with a relationship manager to get real time updates on the service. Customers can also opt to pay the service bill online through the app and can request the vehicle to be delivered to a specific address.

- **SYOUV:** The SYOUV platform is designed to help a customer who is currently in the pre-purchase phase. It provides a collection of important information regarding a Mahindra vehicle. It also offers personalized recommendations based on the customer's actions on the platform. A feature named 'Talk to Expert' allows customers to get answers to their queries in real-time through audio/text chat. The '3D Discovery' shows various features of a Mahindra vehicle in a rich 3D format. There is also a 'Collaborative Exploration' feature on offer through which, users can invite their friends on Facebook and email to collectively customize Mahindra vehicles.

AI takes cyber security to a new level for HDFC Bank

THE CAPABILITIES of current security technologies coupled with the power of Artificial Intelligence (AI) will take the cyber security preparedness to the next level, says Sameer Ratolikar, CISO, HDFC Bank, highlighting his bank's AI based Cyber Security Operations Center (CSOC)

Artificial Intelligence is explored for information security because there are questions raised about the effectiveness of the currently available solutions to thwart the attacks which are becoming more sophisticated, innovative and targeted.

AI can complement with the current security solutions and decipher the anomalies, which are non-signature, behaviour and heuristics based. For example, the security logs in the Security Incidents and Events Management (SIEM) can only serve a limited purpose; however this data coupled with AI solutions has the potential to detect the anomalies, threats which are sitting latent in the system, waiting for the right time to hit. Another use case can be finding trends on the amount of file uploads on PCs and search for aberrations. AI can also team up with other solutions to bring to the fore any divergence in terms of the times during which the applications are accessed by the employees and how can it be detrimental to the company. AI and Machine Laerning (ML) will achieve objectives, not yet achieved by the current solutions, which are reactive in nature.

HDFC Bank has completed a pilot for AI based Cyber Security Operations Centre (CSOC) and soon, the bank will go live. The log data from CSOC is put for processing on the AI solution having big data capabilities and it was done for about eight months on a cloud platform. The bank has close to 100,000 employees. The AI solution will help in monitoring insider threats. The aforementioned anomalies were successfully found using the AI platform during the pilot.

AI has deep learning (DL), self learning and machine learning (ML) as major components. There are well established algorithms in each of these areas. One team will manage the CSOC and the second team will focus efforts for threat hunting by writing rules for ML. The bank will have 70-80 per cent contribution from the vendors and close to 20 per cent from the internal teams. CSOC is a combination of SOC, threat hunting, breach readiness teams, threat aggregation platforms, red teaming, etc.

"Dark web monitoring is a part of the overall security. We are working on dark web solutions, like real-time defacement and vulnerability monitoring. The solution should have features like early detection of malware presence; in case any data is available for sale in the dark web, how soon are we able to know about it," states Ratolikar.

The economics of security

CISOs will have to balance the budgets to focus only on their crown jewels. The company's residual risk and cyber risk tolerance level will have to be identified. However, that said, banks are a regulated entity. The relationship with the customer is heavily based on trust. Thus there is consensus among the bank CISO community that the reputation risk is also equally important. As a result, even the risk tolerance levels have to be continuously tightened.

The investment in cyber security is determined by the risk management principles. Proper controls are put in place after doing regular threat and risk assessment exercises. Adequate investments should be made based on the kind of threats and risks faced by the organisations. If required, heavy budget allocations must be made. Cyber security is a business risk and it has found its place in boardroom discussions too. The importance given to cyber security in banks is way ahead than in any other industry. "We have also found companies paying ransom when their crown jewels are locked by a ransomware. But there is no certainty that the data will be released after the ransom is paid. Neither is there any assurance that the systems will not be attacked again," mentions Ratolikar.

HDFC Bank has completed a pilot for AI based Cyber Security Operations Centre (CSOC) and soon, the bank will go live

Importance of cyber security framework

The concept of perimeter security has collapsed with the onset of API banking. For payment enablement, banks have to talk to government agencies, payment aggregators, corporates etc. When banks are interfacing with hundreds of third parties, the idea of perimeter has vanished. Banks should have an ideal cyber security framework.

HDFC bank's approach is to have a four point - Prevent, Detect, Respond and Recover framework. To have multiple preventive controls that covers the entire ground in terms of the channels through which the customer is served or the bank operates internally or with the third parties. Deception technology is an upcoming space in the detection piece. It's a honeypot created for the hacker. The technology serves the purpose of knowing well in advance about who is trying to target the information infrastructure of a particular organization, and how it's done. For example, create a honeypot for credit card and debit card numbers. This way, the potential hacker is lured to hack the duplicate card registry. The system triggers an alarm after the hacker attempts to get the information, which actually is not a genuine database but a honeypot. After the detection comes the response. There are enough systems in place to quarantine the attack and invoke the DR, in order to mitigate the damage.

Too much focus on prevention is unfruitful because there will always be functions that will have residual risk; for eample, USBs used for cheque truncation is a risk. There are chances of malware getting infiltrated through them, given that there are thousands of employees. Even if a single employee clicks on the infected mail, the network can get affected, through open shares, privilege escalations, with the threat vector, which can be an APT attack, ransomware, etc. This can affect the crown jewels too.

The last part is to recover, which majorly deals with DR and BC, where the Recovery Time Objective (RTO), Recovery Part Objective (RPO) come into play. For the crown jewels, there has to be a file, storage based and database backups. This is a part of the recovery strategy, where BCP and DR is an integrated component. Managing security at an ecosystem level IDRBT, every quarter organises CISO forums, which is well attended by the CISOs from major BFSI institutions. It is developing to be a good platform to share thoughts on the challenges faced, and the developing threat vector scenario. This apart, there are various informal forums, where selected CISOs meet to exchange thoughts on the impending issues. The CISOs also get multiple advisories and presentations from IDRBT. A consortium of banks can come together and leverage ML for information security. The decision whether to join such a consortium depends upon the priorities of each bank.

QUESTIONS ASKED ON CYBER SECURITY IN BOARDROOM DISCUSSIONS

- What is the cyber security preparedness to counter ransomware and from other emerging threat vectors?
- What if we would have been attacked with a threat similar to the one faced by a MNC this year ?
- What would have been our preparedness ?
- The impact on us, the extent of damage faced ?
- What would have been our strategy to mitigate and come back strongly after the attack
- Questions pertaining to IT security budgets are also asked. If at all, what is the scope to enhance the IT security budget to safeguard the crown jewels ?
- Which are the vulnerable areas which can potentially be attacked and is there enough visibility on those areas ?

"Too much focus on prevention is unfruitful because there will always be functions that will have residual risk

Sameer Ratolikar
CISO, HDFC Bank

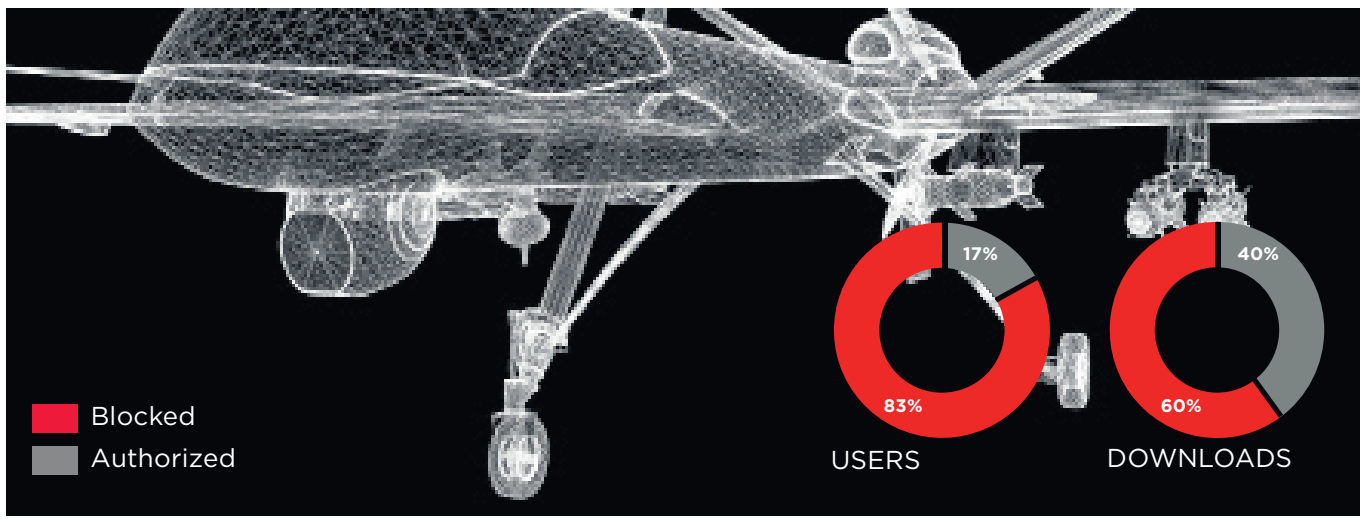
Securing SAP data of a premier Indian defence research center

THE CRUCIAL SAP data of India's premier laboratory of the Ministry of Defence, Research Centre Imarat, is being secured through a slew of advanced security solutions

Research Centre Imarat (RCI) is a leading laboratory of the Indian Ministry of Defence. The immense importance this institute has for India's security is witnessed in its invaluable contribution towards the development of several state-of-the-art strategic and tactical missiles.

To streamline and to improve internal operations, the institute leverages information technology to a great degree. To break operational silos and to integrate vital processes for a seamless throughput, they use SAP as their central solution for Enterprise Resource Planning (ERP). This is where all the sensitive and strictly confidential data of the organization is stored and processed. Before HALOCORE was installed, multiple users across functions not only had access to the center's Purchase Order (PO) transactions, but also had the capability to download or even print copies of the confidential documents. That increased the risk of data loss and misuse, which can not only affect operations of the research center, but also the national security of India.

To make sure that the highly confidential data do not leave the organization and to close the security gap between the SAP system and its users, best-of-breed solutions, such as HALOCORE, were in demand.



Restricting access: How HALOCORE stemmed free flow of SAP-based purchase order data (6 month period)

The solution

After a string of discussions, demonstrations and a pilot project to gauge the solution's performance within the operational environment, RCI decided to implement HALOCORE – currently the only ideal solution for such demand in the market.

The modules BLOCK and PROTECT allow security managers to classify SAP data and to assign fine-grained rights for access, download and printout of confidential purchasing data – without affecting the legitimate access permission to SAP transactions. Besides that, HALOCORE encrypts all data that is needed outside of SAP and protects it against misuse - even if users insert them into Microsoft Office documents or other office files. The protection requirements of such data are transferred automatically. Moreover, the organization uses the module MONITOR to supervise and document all export and print operations and to be able to react quickly in case of a security incident.

This innovative and SAP-integrated approach allows RCI to maintain a high level of control and securityover sensitive data and documents extracted from SAP. They are able to block data that must not leave SAP and to protect data that is required outside of the SAP environment.

The result

With HALOCORE, RCI was able to limit the number of users that are allowed to extract data from the SAP system, from more than 100 to just 20. At the same time the security solution ensured the ability to precisely report all export and processing details. Over a time period of 6 months, HALOCORE has already blocked more than 1,800 unauthorized downloads.

In the coming months the solution will be extended across all other materials and finance processes of RCI. Also, as a chosen data security solution for the SAP landscape, HALOCORE forms an integral part of DRDO's plans to expand SAP use across associated institutions.

"We are in a very serious domain – National Security. Naturally, we take extreme precaution to protect our data inside and outside our premises. With HALOCORE, we are now doubly reassured that sensitive information relating to our order management is secure and remains so – despite multifarious threats."

Gautam Mahapatra
Director Technology & Systems, Research Centre Imarat (RCI) Defence & Research Development Organisation (DRDO)

ABOUT RCI

Research Centre Imarat (RCI) is a leading institute of the Defence Research and Development Organisation (DRDO) and pertains to the Indian Ministry of Defence. The center is located in Hyderabad, Telangana, and is responsible for the research and development of missile systems, guided weapons and advanced avionics for the Indian armed forces.

KEY TAKEAWAYS

- Control over all SAP data exports and their further processing
- End-to-end protection of confidential SAP data
- Minimalized risk for breaches, data theft and accidential loss

SUCCESS FACTORS

- Intelligent data classification
- Strong data encryption
- Granular rights management that hones SAP Standard and SAP GRC

HALOCORE'S USP

- Blocking data that must not leave SAP
- Protecting data that is needed outside of SAP
- Monitoring data that is exchanged between SAP and nonSAP systems automatically

Shiv Kumar Bhasin,
CTO, SBI

How emerging technologies such as Blockchain, IoT and RPA are making an impact on cyber security

#1 Blockchain

Blockchain implements strong security technology that provides integrity, availability and mutual trust, but not confidentiality, across enterprise boundaries with no central arbiter. The distributed nature of blockchain technology that goes beyond organizational boundaries makes it difficult to assess a use case at hand is best solved with blockchain security features or by a combination of conventional security tools.

Even though a blockchain network is considered to have no single point of failure, organizations could still face risks from external events outside of their control. For example, a global internet outage would disrupt even a public blockchain network as distributed as Bitcoin or Ethereum, creating outages which would impact an organization's operations as with any other technology. Private blockchain networks with a lower number of nodes would need to ensure that their network is sufficiently distributed globally and resilient with no single points of failure on an organization or platform level to ensure continuous operation even in the event of a natural disaster or coordinated attack

In the current generation of blockchain technology, there are insufficient privacy controls. In public blockchains, the sequence of events and activities, such as the execution of smart contracts, is recorded, propagated to all nodes and visible in public. To date, blockchains, such as Bitcoin, are "pseudoanonymous" using the hashed public keys of the parties as pseudonyms, while other data, such as the date, time and amount of the transaction associated with that event is publicly visible. Events can be any event related to your use case; for example, in digital currencies they are transaction amounts and updated account balances.

Blockchain-based architectures can help address many security issues, and we'll see more blockchain-based initiatives around fraud management and identity. At the same time, developers and security professionals will pay much greater attention to the security risks posed by interfaces with existing systems, serious software bugs, and potential future risks posed by quantum computing.

Whitelist, blacklist, and previous transaction-based information — retrieved from blockchain-backed, tamper-evident sources (think of these as the next-gen EWS or OFAC) — will enable banks, insurance carriers, and e-commerce retailers to much more effectively combat financial crime. Any organization subject to regulatory anti money laundering (AML), know your customer (KYC), identity verification (IDV), and enterprise fraud management (EFM) mandates has struggled with these requirements to adequately vet and monitor its user population for identity theft and suspicious activity.

Blockchain data sources and future

Blockchain will become a foundational technology for: 1) certificate issuance and authentication; 2) IDV; 3) malware and ransomware protection via binary reputation checks; and 4) document authenticity and integrity verification.

Blockchain is a nascent technology and attackers will find more ways to tamper with blockchain data and services. Some of the known risks include: compromise of encryption keys, software deficiencies and vulnerabilities, loss of encryption keys, legal compliance risks, market adoption risks, governance risks, smart contracts with malicious terms, lack of scalability due to unforeseen issues.

#2 IoT (Internet of Things)

No IoT device should be able to communicate on the internet without forcing the end user to change the default password. Manufacturers should randomise default passwords based on a few factors such as date of manufacture, serial number, and distributor. Devices should also come with a strict egress filtering policy that limits where they can communicate. For example, unless the user updates the configuration by default, the device should only be able to communicate back to sites owned by the manufacturer. Firmware updates should be signed with a digital certificate. Unfortunately, none of these best practices are common practices today.

There is a plethora of IoT standards and protocols, which creates security blind spots. Today's IoT ecosystem is a complex web of industry-specific devices and use cases that use a wide range of communications protocols (such as AMQP, CoAP, and MQTT) to enable edge devices to communicate with gateways and cloud services, as well as with different data formats and software interfaces/APIs. This fragmented approach creates interoperability challenges when integrating multiple IoT-enabled devices into any existing enterprise architecture. These interoperability challenges breed complexity and increase security threats and vulnerabilities due to difficulties in applying consistent security policies across all devices and protocols.

While IoT scenarios face similar security vulnerabilities as the traditional desktop universe, the sheer number of IoT devices dramatically increases the scalability requirements. These scale requirements may trip up traditional security solutions that try to extend into IoT scenarios or require additional hardware investment, which will make such approaches economically unfeasible. Those IoT security solutions that can prove the ability to handle scale will ultimately realise greater market penetration and success than those that don't scale.

There is a lack of clarity of responsibility regarding privacy and security. Managing identities of IoT devices is a critical piece of the IoT security puzzle. Unfortunately, in many IoT scenarios, security responsibilities can be unclear (is it the device manufacturer, the network operator, the app provider, or all of the above?). This lack of clarity requires that developers of IoT-connected objects design appropriate privacy policies and data handling into the device, with explicit instructions on how users can opt out of data sharing as well as explicit descriptions on data usage, storage, and sharing. S&R pros also face different country-specific data privacy regulations about requirements to collaborate with their legal and line of business counterparts to develop a multi-faceted approach for managing IoT data privacy.

Encryption is an absolute must. In IoT scenarios, encryption (whether on the data, the network or both) is an essential IoT security best practice. And although encryption is necessary to meet the usual requirements around personal privacy and confidentiality, many IoT scenarios now involve automation of industrial, business, and personal processes. This may create business value, but it also introduces scenarios where breaching of these IoT systems can lead to destruction of property and equipment and even personal safety issues. The higher potential risks associated with IoT scenarios mandates encryption of data in motion and at rest and that the security team maintain appropriate key management processes and procedures to ensure integrity of the encryption keys.

#3 RPA (Robotic Process Automation)

Given that RPA is an emerging technology in the service industries, there are no standards or formally agreed upon industry controls specific to RPA. Indeed, this has been given little focus to date as the drivers have been around cost reduction and the adoption has been modest to date. There seem to be two starkly different ways that people think about automation and cyber security. While some believe that bots are basically invulnerable, since they never deviate from rules and are immune to the kind of curiosity that makes you click on a phishing email, others have nightmares about increasingly smarter robots going rogue on their networks, making them resist RPA altogether.

Suddenly, your bot doesn't do what it's supposed to do. It's a fearful scenario that can be panic inducing. What do you do? Well, you obviously unplug it, but don't leave it at that. There's a reason the bot lost its mind, and it's not because it has one of its own. You have to go back and reconstruct what happened (i.e. malicious or change in code/business logic or not appropriate change management or other misuse by an employee), which is why it's so important to make sure that you have an audit log that records all activity.

RPA is often promoted as a solution that can be deployed independently by a business unit. But like any other software solution, the IT and the information security departments must be critical stakeholders in planning, deploying, and managing the solution throughout its

Bharat Panchal
SVP & Head, Risk Management, NPCI

Understanding the relevance of cyber security in the BFSI sector

Protecting sensitive data is important, industries across the globe agree on this fact. With surmounting pressure on CIOs and CISOs on putting higher investments for security infrastructure, the challenge of facing sudden attacks on protected data and customer information is getting bigger and more unpredictable. During the time companies and leaders were discussing the optimal budgets to spend on building a resilient, secure infrastructure, the perpetrators were not sitting idle. Newer technologies and enhanced software knowledge has today led to major data breaches across the world. India is also not different than the rest of the world in terms of cyber security breaches.

While secure data makes for the basis of a successful business in this connected world, building consumer confidence on your security architecture is only one angle to tackle. The bigger challenge lies in creating an ecosystem that not only promises to be safe and keep critical customer data safe, but also comes together in understanding the constant need for vigilance. With everything else, hacking has evolved too. It calls for an industry-wide stance where irrespective of the threat, organisations are safeguarding their data and building robust strategies to mitigate security risks and improve crises response time for difficult situations.

Protecting valuable data

Having discussed the need for information and data security structures in place, let us not forget that it is not only banks or financial institutions who are in need for mitigating data breach situations. Every company and organisation needs to protect its valuable data to maintain business continuity. However, the impact of a breach is often seen manifold for the BFSI sector because of the sensitive nature of customer's financial data. Conventional data protection is just not enough for the current reality. Companies need to think deeper into the possible consequences of a data breach and strategise their security infrastructure accordingly.

Stringent security practices

Securing technology systems and protecting the data and assets of customers remains one of the highest priorities for any financial institution. Evolving security threats, both internal and external, require the use of new controls, latest methods and sophisticated advanced security tools to protect all transaction activities and data. Multifaceted and layered security tools and procedures strengthen any institution's efforts in combating against these threats by providing multiple automated barriers at different levels. Hence, it is important to ensure that security practices are stringent by utilising a strong, multi-layered security strategy, including the use of best of the security tools like firewalls, proxy servers, SIEM (Security Incident and Event Management), two- factor authentication with tokens, PIM (Privilege Identity Management), FIM (File Integrity Management), WAF (Web Application Filtering), APT (Advanced Persistent Threats). In the banking and payment system, a strong security strategy requires that all high-risk transactions be reviewed and authorised by the customer, and that the payment system network uses industry-standard practices to validate the legitimacy of those transactions. A layered security policy should also take into consideration where sensitive data is stored, human resources, and the physical assets of the organization, including laptops, tablets, printers, scanners, mobile phones, Wi-Fi and access to all other facilities.

Type of challenges in Cyber Security:

- Mobile Banking
- Malware, botnets and DDoS
- Phishing
- Skimming
- Strong controls for mobile browsing and apps

Indian banking industry has successfully enabled mobile banking for large customer bases. The process is long and enduring, as the traditional online banking security infrastructure and measures do not always apply to mobile banking as it is. As customers get the liberty for anywhere, anytime banking, it is imperative that strong controls are put in place for mobile browsing as well as the apps by the security managers and experts. Similarly, there are challenges from extensive malware attacks, phishing etc, which has extensive impact on the reputation of the bank/financial institution much more than the benefits it takes out of a successful perpetration.

Much has been spoken about the various kind of challenges in the sphere of data and cyber security. An organization's cyber vulnerabilities extend to locations where its data is stored, transmitted, and accessed, both by organisations and its service providers. Any weakness in the perimeter becomes the organization's vulnerability. This challenge will continue to increase as the organization's cyber security perimeter continues to expand as customers increase their demands to allow access to their information irrespective where it is stored.

Best practices of cyber resilience standards

Any organization should implement adequate protective controls that are in line with best practices of cyber resilience standards to reduce the likelihood and impact of a successful cyber-attack on identified critical business functions, information assets and data. Protective controls should be proportionate to and consistent with the organization's risk tolerance and its threat landscape.

Integrated crisis response system

The need of the hour is an integrated crisis response system that evolves itself with newer challenges by creating a perfect amalgamation of people, processes and technology. It is crucial for businesses to maintain continuity even in case of an attack, and to get back on feet within a quick turnaround time.

In a dynamic industry such as banking and finance, where core banking systems and new technologies work hand in hand, the payments systems where technological innovation is paving the way for digitalizing whole economies across the world, advent of new and faster ways of banking on the go, security will always be of utmost importance. Prevention is hypothetical in today's business environment since the hackers are finding new ways of turning what used to be a show of power, to a money making crime. The question is how organizations ensure getting back on feet once perturbed, to deliver the same confidence they have in their systems to the customer.

Strategic governance and strong deployment of tools

Adopting a preventive approach to tackling cybercrime related risks could help to enhanced security with improved value. However, it typically requires a paradigm shift that starts with high level governance strategy to incorporate cybercrime related risks into the enterprise risk strategy. That will help to start to identify gaps in the current cybercrime risk management strategy and encourage an organization-wide approach to countering cyber threats. Further, along with the strategic governance, a strong deployment of tools is very much necessary as a preventive approach towards cybercrime risk management.

Indian telecom sector: Top five cyber security risks

FAILURE TO ADHERE to regulatory requirements; cyber attacks disrupting telecom services; subscriber data privacy breaches; cyber security function's inability to support new business initiatives with equal pace and finally concerns associated with outsourcing are some of the risks faced by the Indian telecom sector. EC's Abhishek Raval discusses them with **Amit Pradhan**, CISO, Vodafone

Which are the top five risks that Indian telcos face?

The top five risks for any telco in India would be the following:

The first risk is failure to adhere to regulatory security requirements and thereby non-adherence to the regulatory regime.

Indian telecom security regulations have some of the most stringent security requirements in the world. These regulations are intended to protect data privacy of subscribers, national critical infrastructure, enable national security, and assist law enforcement and intelligence agencies to provide a safer environment for the citizens. Some of these requirements include appointment of a CISO who is an Indian citizen; all critical telecom devices be managed by only Indian citizens; subscriber data to reside and be accessed only from India and nowhere outside India; telco operator to seek approval/declaration for all deviations, etc.

Failing to demonstrate compliance to these requirements may attract suspension or cancellation of license. In case of a data breach, if the operator is not able to demonstrate adequate security controls as per the compliance, the operator may be subjected to financial penalties of upto ₹ 50 crore per license, per breach. Which means, considering a massive data breach across all licenses, the amount could go in multiple of ₹ 50 crore, based on number of breaches, with multiple licenses (approximately each operator has 26 license). The amount subjected may go up to ₹1,300 crore hypothetically.

The second risk is breach of subscriber data. A telco has personal and sensitive information of millions of subscribers. This information include their birth date, residence address, PAN, license, Aadhaar number, all data records, their location, etc. While most of this data is not available to any individual in the organization, some of the data is required by the law enforcement agencies during criminal and national security related investigations. It is the telco's primary responsibility to build a strong and secure environment to store, process and move this data as and when required by government agencies. Loss of this data due to a data breach would mean, telcos can lose their reputation, subscriber and stakeholder trust, ultimately resulting in loss of current and future business revenue.

The third risk is that of attacks from cyberspace. A telco has a massive and complex technology environment. Distributed Denial of Service (DDoS) attacks have been quite prevalent since the last couple of years and have known to disrupt services across financial sector. There was an FIR filed (first-of-its-kind) by a company, last year with the Mumbai cyber police against an unknown attacker for perpetrating a DDoS attack to scale of 140 Gbps. These attacks appeared to have originated from China and Eastern European countries. The attackers use telcos as conduits for carrying out the attacks. Thus they play an important role in keeping the industry safe. Especially, the BFSI, power grids etc, which take services from us.

> The eKYC process has not only improved the customer experience in getting a connection but also improved the overall security posture of the setup

The fourth risk is the inability of the cyber security function to support the business in the rollout of new innovation initiatives on the business side. This involves exploiting different technologies to roll out new customer services. When the telecom industry is moving from voice to data, and with new technologies also coming in, sky is the limit, on the amount of offerings that can be coined. It is the CISO's function to make sure these services are launched after right security controls are taken care of. Security has to be covered from all the angles - in the stages of design, implementation and post implementation.

The inability of the CISO to deliver will result in telcos failing to respond to competition faster and will also affect the competitive edge.

The fifth is the risk involved with outsourcing. Majority of the functions of telcos are outsourced. Most of the staff is not on the direct rolls of the company. The companies to whom we have outsourced also in turn sub contract their jobs to other companies. The huge database that we have is managed by these complex web of outsourced companies. The control that I can exert on my employees cannot equally be applied on the employees of an outsourced company. Hence it is important to establish the right checks and balances while outsourcing and managing the outsourced partners. It is important that all necessary security requirements are included in the contracts and SLAs with the partners.

How do you make sure information security is handled at the level of the kirana shops / retailers that give out new connections and provide recharges?

A major challenge in engaging with the retailers is in the process of issuance and management of new connections to the customers. To get a new SIM card, the customers have to give out their personal details in the client application form given by the telco.

The retailers and kirana shops provide SIM cards to the subscribers. The SIM cards are mapped to our system. The only transaction that retailers can do is 'recharges'. The recharge limit is set for the retailers based on the business volume they garner for the telco. These restrictions save us from potential financial losses. The revenue assurance and fraud risk and security team continuously keeps track of these transactions. Alerts are triggered when anomalies are found. Investigation begins when a certain threshold is breached.

In the light of security, how do you distinguish Aadhaar enabled KYC and the process followed earlier?

A subscriber earlier would need to provide his proof of identity, proof of residence along with a customer information form to apply for a connection. Post the physical verification, the SIM card would be activated. With eKYC being adopted (in metros/few other locations), the customer can visit a store, fill up the form and get his SIM card activated in minutes after using biometric authentication. The eKYC process has not only improved the customer experience in getting a connection but also improved the overall security posture of the setup. Unlike the earlier time, where it would be difficult for a store manager to verify signature, authenticity of documents submitted and overall security in protecting these documents, with eKYC the receipt and storage of these documents can be avoided. Additionally, the store manager, through eKYC, can be assured that the customer has provided correct and accurate information.

How do you view the application of Artificial Intelligence in cyber security?

AI provides a major potential in the field of cyber security. The first use case can be in security prediction for cyber-attacks and frauds which can help organizations prevent fraud instead of responding. All frauds and anomalies have characteristic behavior, which cannot be assimilated by a human due to its large volume. AI can play a critical role here.

The performance of the telecom networks can also be improved using AI. For example, call drops. If AI is made to understand the various reasons due to which calls get dropped, it can result in a huge revenue earner.

User profiling and anomaly detection through advanced analytics and AI can help identify individuals (disgruntled employee, employees who have resigned, etc) to help alert the security team of possible data leakage or unauthorized usage. These combined with restrictive mechanism may actually help block an authorized user who has resigned and is trying to pull confidential information out.

CISOs should articulate the cyber risk to the top management

CISOs ARE BEST suited to articulate the cyber risks faced by their organization to their leadership and board. Therefore the CISOs need to be positioned at strategic level by the organizational leadership so that all important cyber risks are tabled for discussion with them and the board. **Vishal Salvi**, CISO, Infosys speaks with EC's Abhishek Raval and explains how CISOs can take the lead in heading cyber security initiatives for the company

Budgets are a constraint that CISOs face. Do you think, across Industries the amount of money that should be allocated to information security is enough?

Getting budgets is the core issue here. In many organizations the CISOs are best operating at an operational level and hence they are not able to surface the top cyber risks to the leadership and the board. As mentioned earlier, organizations need to invest in CISOs and position them to operate at a strategic level.

In today's world, you cannot think of any organization without digital push and online presence. The dimension and size of the cyber risk faced by the organizations is based on the nature of their business, their industry and the size and scale of the organization. Large organizations know that managing cyber risks is important and are willing to invest, so long as they are able to understand them better and also know the impact to their business in case they materialize. Proper articulation of cyber risks is an important part of the CISOs role and sets the tone of how cyber security is practiced with an organization.

At Infosys, the CEO is the chair of the Information Security council. You can't get bigger sponsorship than that. The board regularly reviews data on how cyber security is practiced and implemented. The same was the case with the organizations that I have worked for in past. The board ensures that there is proper visibility, cadence and governance around the cyber security program. The question is, in how many organizations, we have such practices being followed. CISOs should not be mere ceremonial; they should be authoritative and independent voice on cyber security, which reaches the leadership and board.

So, should the CISO position himself or the management should empower him and give the required headroom?

The hiring of the CISO and the positioning can't be done by the CISO himself. The leadership in the organization has to drive this. If that's done properly, it's half job done. The second part is the empowerment of the CISO. The role should be independent of any conflict of interest, should be empowered to raise issues and risks to the leadership and the board. There are a lot of other aspects, such as influencing, change management, technical acumen etc. These are important attributes that every CISO must have.

In short, lack of security budgets is just a symptom. The root cause is, there is nobody senior enough to articulate the seriousness of cyber risk issues to top management, for the money to be allocated.

What techniques would you suggest to CISOs to get their voice across to the top management and be independent to position themselves?

> Any platform set up for information sharing is always useful to collaborate and act on certain issues, incidents and imminent threats proactively than learn from personal experience

- Articulating the risk and integrating with the risk management framework to provide a convincing business case to get funds
- Quote examples of recent cyber security incidents to explain the risk
- Explain the current cyber security status compared to the peers
- Building a good cyber security strategy
- Stakeholder mapping, engaging with the right stakeholders and regular interactions with them to influence them to support the organization's cyber security program
- Do internal assessments; identify control failures and gaps and show where we are and where we ought to go. Connect it with risk management in such a way that cyber security doesn't become a problem but becomes an enabler for business

You have worked in various roles - as a banker and then CISO of large bank, as a Partner in one of the Big4s and now as a CISO and SVP at one of India's top IT services company, Infosys. Please share the learnings?

The experience at Standard Chartered Bank as Head, Office of Information Technology Services (OITS), exposed me to global perspectives and processes. Being a purist British Bank, cyber security was always high on priority. It particularly helped me to imbibe the best practices on the security side of banking. As the practices learnt at the bank were globally acknowledged for their effectiveness, they came in handy during my stint at HDFC Bank, which is a large local bank in India. It was especially useful at the bank, because I was playing a leadership role and we were setting up and stabilizing the security operations and also simultaneously working on transformation initiatives.

The Information Technology Governance Risk and Compliance (ITGRC) project in HDFC Bank was completed in two years. However, the same project was implemented in just six months at Infosys. It was because of the lessons learnt at HDFC Bank.

At my two-year stint in PwC, I got the opportunity to talk in depth with close to 100 CISOs in their office. This was a totally different experience and knowledge gathering that happened compared to sitting in office and trying to understand what our peers are going through. These meetings help to infer on why the execution of certain aspects of an implementation fails; where organizations fail in delivering certain services.

Having worked in different roles has given me this sense of empathy towards my stakeholders which is so valuable in implementation and execution of our vision.

How do you see the development of the concept of collective effort, and ecosystems coming together to fight cyber crime. For example, life insurance companies have formed a consortium to share threat related incidents. Sectoral CERTs will be formed soon. What's your view on multilateral arrangements and consortiums to fight cyber crime?

There are established models of information sharing, practices. Financial Services Information Sharing and Analysis Center (FS-ISAC) in the USA is a good example. The organization started off for the financial sector and it has branched out to sectoral ISACs. It was formed in around 1998-99, but it took them about a decade and by 2007-08, they became more effective. They are not-for-profit and funded by various sectors. While there is a body and core committee to run the organizational operations, it's the member organizations who are contributing to capability building in information sharing.

On the same lines, the Government, under the National Cyber Security Coordinator's office, had initiated a joint working group, in terms of what needs to be done. I was a part of the joint working group responsible for Information sharing for the financial sector.

Any platform set up for information sharing is always useful to collaborate and act on certain issues, incidents and imminent threats proactively than learn from personal experience. More needs to be done. While there is some progress that has happened but we can do much more than what we have in place right now.

Which are some of the use cases for the application of AI in cyber security?

In some areas AI and ML are already operational. There are use cases for using AI in the Cyber Security Operations Centers (CSOCs). The traditional tools in a typical SOC are currently unable to solve the same problems.

The Security Incident and Event Management (SIEM), security analytic tools have been around for quite a few years. They have delivered well, however, with certain limitations. AI and ML can solve those problems; for example, inputs from threat intelligence and asset inventory, incident management can be consolidated and an AI model can be run over it to make reasonable predictions on certain events that might happen on the network. While a part of it is possible using SIEM, a majority of this problem can be solved by AI.

The issue of false positives has plagued the cyber security world for many years. Infosys is incubating and testing models on how AI can be useful in segregating false positives from the suspicious traffic.

Our objective is to democratize AI

DISCUSSING THE IMPORTANCE of AI, **Prakash Mallya**, Managing Director for South Asia, Intel, in an interaction with EC's Rachana Jha, states why Intel is bullish about India's market potential, and highlights the company's efforts in making 5G a reality in India

Some edited excerpts...

What have been some of the major initiatives that Intel has taken in the past one year?

We see tremendous opportunity in the growth of cloud and data centers, which makes India a strategic region for our growth, contributing significantly to Intel's technology and product leadership. Perhaps our biggest asset is our dual ability to develop a full suite of hardware, from robots to drones, as well as define the network infrastructure build on cloud and data centers, upon which these technologies operate. This is why our strategy is to transform from a PC-centric company to a data-centric company.

Our leadership under the data center group business in India pivots on high performance computing (HPC), Artificial Intelligence (AI) and cloud and analytics. In India, we see potential in the BFSI, telecom, and e-commerce sectors, across big data, and Internet of Things (IoT), which are complementary to HPC and AI. In fact, there is already an uptake in the HPC segment among the academia and local customers, including the National Stock Exchange (NSE), and cloud service provider NxtGen. We have recently introduced the Intel Xeon scalable processor family platform, which will provide a foundation for AI, HPC and cloud. Earlier this year, we also hosted the India edition of our global AI Day, to showcase the companies that are effectively using M2M learning to make nimble business decisions, the solutions that hold potential for India, and Intel's commitment to making that happen. 15,000 developers are already being trained under this initiative, and it won't be long before we start seeing the real impact.

How do you see the evolution of the IT industry in India?

The IT industry in India is witnessing a sea change with the advent of new-age technologies such as AI, big data analytics, IoT, as well as digital-first policies such as the now implemented GST and the 5G proposal.

We are building the next generation of these technologies, which puts us in a unique vantage point to help drive the future of the country's fourth industrial revolution. Given our presence at the edge and at the data center, we can ensure a seamlessly integrated and secure IoT environment combined with our processor capabilities. With our expertise and assets, we are focused on AI, 5G, IoT, and HPC, all powered by cloud-connectivity, to enhance the value proposition we bring to our customers here through Intel architecture. In that sense, we are uniquely positioned to deliver insights from data, which in turn is driving innovation, releasing new services and businesses back into the Indian economy.

What opportunities does Intel see in the enterprise space in India?

We see tremendous opportunity in the growth of the cloud and data center, IoT, memory, and FPGAs, all bound together by connectivity. It's important though to realize that connectivity is not just about connecting every phone in the world. There are eight billion people, so potentially there are eight billion phones. But one of Intel's drives is to connect 50 to 100 billion things. If you look at the portfolio of the connectivity technologies that we're putting together, they're driving an entire panorama of devices, the phone being only one category.

Additionally, the government's 'Digital India' mandate makes us twice bullish about India's market potential – especially in sectors like BFSI, telecom, and e-commerce for solutions in HPC, big data, and IoT, all of which are complementary to AI. As mentioned earlier, there is an uptake in the HPC segment among academia and local customers.

We are working on establishing deep industry collaborations and power skill building to promote the adoption and usage of AI. With reference to 5G, we are focusing on three key areas: industry partnerships, end-to-end 5G-related hardware / software, products and platform, and supporting 5G standards-setting. Here we are working with the Department of Telecom, to provide it with information from studies and trials, which in itself is a first. And, finally we are exploring the possibility of setting up test beds and taskforces on both sides to work towards making 5G a reality sooner than later. Intel is also bringing innovative technologies in the realm of high performance computing for partners to build solutions and lay the foundation for a digital infrastructure in the country. The Intel Xeon Phi processors launched last year enable complex tasks and support highly scalable workloads in science and technology research. The opportunities

> We have supported the government to establish 10 of the 500 Atal Tinkering Laboratories (ATL) , as a blueprint for the facilities where students will gain hands-on experience with chips, boards, robots, and machines, to experiment and engineer their own mini machines

are immense for the HPC market in India and the uptake is only going to increase in this market. Last but not the least, there is cloud computing, adoption of which is getting a boost from India's fast growing tech startup ecosystem – as these businesses evolve, they are likely to invest more in their IT needs such as purchasing high-end servers, effective software tools, database licenses. Also, most of these 'cloud-born' startups opt for software based services since these are highly economical and can help new enterprises perform efficiently with fewer resources.

What is Intel's strategy, specifically with respect to AI in India?

Intel has aligned its AI strategy for India in line with the government's rapidly evolving Digital India vision and is making major investments in technology, training, resources, and R&D in AI. We have established deep collaborations with Hewlett Packard Enterprise, Wipro, Julia Computing and Calligo Technologies to accelerate the onset of AI. Additionally, we rolled out a comprehensive Intel AIDeveloper Education Program in India which is targeted at educating 15,000 scientists, developers, analysts, and engineers on key AI technologies, including Deep Learning and Machine Learning.

Through 60 programs ranging from workshops, roadshows, user group community and senior technology leader roundtables, our objective here is the same as our global AI objective – to democratize AI by addressing three basic challenges; lack of vocational skills/relevant workforce through developer engagement/education program, bring together the scattered ecosystem through local partners who can develop relevant solutions, and enable knowledge sharing and address the technology requirements for academia and research by working with institutes such as IIT Patna, C-DAC, IISC, to drive more opportunities for AI, each of which is enabling social impact. Also, we recently hosted the first India edition of our global AI Day.

In August this year, we launched the Movidius Neural Compute Stick, the world's first USB-based deep learning inference kit and self-contained AI accelerator in a small form factor. We are excited about its capacity to deliver dedicated deep neural network processing capabilities to a wide range of host devices at the edge. Designed for product developers, researchers, and makers, the Movidius Neural Compute Stick is designed to ensure developers are retooling for an AI-centric digital economy.

Is Intel also engaged in any government project currently?

Yes. As mentioned, to expedite the roll-out of 5G, we are supporting 5G standards-setting by working with the Department of Telecom. We have worked with NITI Aayog under its flagship program, Atal Innovation Mission (AIM), to set up the Tinker Lab concept for 'mini makers' in India's middle and high schools. We have supported the government to establish 10 of the 500 Atal Tinkering Laboratories (ATL), as a blueprint for the facilities where students will gain hands-on experience with chips, boards, robots, and machines, to experiment and engineer their own mini machines. Currently, we are running our Future Skills Program at the labs, under which we are training 900 underserved, high-potential students in digital literacy and tech skills. The idea behind the program is to raise an 'innovation generation' which has the design mindset to create new tech innovations that respond to the community, government or personal challenges. Ten labs are spread across the country, from Assam to the Andaman and Nicobar Islands, and across girl's schools, public schools and army and air force schools. So far, we have engaged 9,369 students at the Pre-Tinker level, of which the majority (57 per cent) are girls.

Entry level professionals lack the right conceptual understanding of cyber security

WITH THE INFORMATION security domain rapidly evolving with changes in business models, technology adoption and regulatory and compliance mandates, it is time to take a new approach for building skill sets in emerging areas. EC's Abhishek Raval speaks with **Sunil Varkey**, CISO, Wipro

Please discuss the challenge of the shortage of cyber security talent in the industry ?

There is a serious shortage of quality human resource in the space of cyber security. There are reasons for the same. Engineering colleges were not offering any courses or specialization in cyber security till very recently. Now, colleges like Vellore Institute of Technology (VIT) have started specialized courses in cyber security.

Most of the available training courses were limited to product specific trainings and on maturity to courses like CISSP, CISA but were limited to role or function specific.

Few years ago, enterprises used to invest in their employees by spending considerably on training, to improve skill sets of their security resources. Post that, few companies started poaching these trained resources, which led to high attrition levels in companies which tried developing skills of their security resources. Overall, this resulted in a reduction in the training spend in companies.

While certifications, trainings and skill development were the key approach in improving employability, recent demand and supply imbalance in the cyber security domain opened up jobs to many without adequate experience or certifications, due to which individuals spending time on reading and upskilling also got reduced.

All this led to a situation where right quality resources with strong foundation, domain expertise, context and perspective started declining. Due to which, these resources are not trying to understand the significance of the role they play, their contribution to enterprise, functional and teams goals and objectives, regulatory and compliance regime, internal and external threat and vulnerability environment, where they are designated to be the protector. This is a global problem in our domain and not limited to India.

> While the importance of the foundational concept of confidentiality, integrity, availability, accountability remains, each of these areas need specialized skill set and approach; and most of these skills cannot be built in isolation

Can the government, corporate, academia, and start-ups come together and build a good environment around cyber security?

The issue is that everybody is waiting for a call from the other party to begin with a common objective. It may not be the right approach.

Nonetheless, compared to the earlier years, a lot of collaboration is happening on the ground. The media is also creating awareness about cyber security. Everything seems to be falling into place.

Innovation and excellence haave come up in various phases from startups. It has happened only after the academia, government and corporates have come together with a common vision and goal.

What are some of the skill sets that will be in demand in terms of cyber security in the coming future?

Information security domain is rapidly evolving with changes in business models, technology adoption, regulatory and compliance mandates, threats, vulnerabilities and exploit patterns.

Overall there are over 20 different functional roles in information security / cyber security domain. While the importance of the foundational concept of confidentiality, integrity, availability, accountability remains, each of these areas need specialized skill set and approach; and most of these skills cannot be built in isolation.

The emerging areas of cloud security, IoT, big data, agile scrum methodology require new learning and approach.

What are your views on the use of data analytics in cyber security?

The AI and ML space is in an evolving stage but for sure big data has picked up its momentum. Currently, security professionals are spending a lot of time on analyzing a lot of events generated from various data sources in the enterprise. We never had the capacity or capability to analyze such volumes of data in the right manner. Now, with the advent of big data platforms, we have better understanding of the patterns, deviations, and triggers to certain events generated in our environment. This helps us in taking informed decisions at the right time.

Now with AI and ML we could get into better threat predictability modelling, which could improve the domain capabilities in a different manner.

Additive manufacturing, AI, ML, edge computing, digital Twins, conversational platforms and blockchain bound to get sharper in 2018

THE NEW FISCAL year will come with a lot of digital transformation and hence it's time for CISOs and infosecurity professionals to set new resolution goals and come up with new trends of cyber security. Keeping in mind the numerous data breaches that occurred in 2017, organizations need to modify existing cyber security approaches and implement new measures. **Bithal Bhardwaj**, Chief Information Security Officer (CISO) , GE South Asia & Africa, in an interaction with EC's Rachana Jha, discusses the journey of the digital world in 2017 and what would be the top trends of 2018

Some edited excerpts:

How do you see the present scenario of digital transformation in the industrial world?

Most global industrial companies today understand that to reach the next level of efficiency and value, they need to connect their assets and plants to take advantages of big data, scalable computing and advanced analytics. The Industrial Internet of Things (IIoT) has become increasingly more pervasive in the industry as digitization has become a business priority for many organizations. It is changing the way industries work. Whether it's enabling predictive analytics to detect corrosion inside a refinery pipe, or providing real-time production data to uncover additional capacity in a plant, or driving visibility and control over your industrial control systems environment to prevent cyber attacks – the IIoT and the software solutions powered by it are driving powerful business outcomes.

Is cyber security a concern for industrial companies undergoing digital transformations?

As more and more organizations connect online to improve efficiency and automation, greater the risk of infiltration, infection and disruption. Unlike traditional data breaches, where it's mostly about sourcing and selling stolen information, cyber attacks on industrial and critical infrastructure are often motivated by malicious intent to disrupt operations, which can place people, property, or the environment at risk.

Many organizations, however, remain unfamiliar with this new and intensifying risk landscape and/or lack insight into how to apply cyber security practices, especially within operational technology (OT) that run these environments.

What measures one can take to mitigate these attacks? What are some strategies to combat such security threats?

Get real industrial security/critical infrastructure expert(s) to come in to evaluate systems and risks in your industrial environment would be my first and foremost advice. Most companies in their early industrial security journey often take misstep of conceiving industrial security as just another IT area to be secured.

Broadly, companies can start with creating a comprehensive security program that understands what needs to be protected. Program should have deep understanding of OT systems, enterprise systems, physical assets, network infrastructure and the dependencies between these components. Consider the possible consequences of a cyber attack to establish the baseline for the security strategy.

The cyber security ownership and responsibilities should be established clearly between the IT and the operation's organizations, under a common leadership. While IT teams focus on protecting data and systems, their OT counterparts must protect mission critical assets and control systems.

Lock down OT systems with right topology and protect with intrusion detection. Right configurations must be applied to protect industrial control systems (ICS) from outside attacks and IT systems should be fortified at the edge of the internet for such environments.

In terms of security, what were the notable developments in 2017?

There are many reports out there outlining major events of the year globally, so let me touch upon just a few things based on media that stood out for me as cyber security professional based in India. Petty cyber crime rate continues to be very high in India with extremely low report rate to the authorities. It can be attributed to high internet penetration with low-end smartphones and lack of security awareness among the masses. Botnet infections in India continue to rise and are among the highest in the world, likely due to a surge in mobile and banking malware. Ransomware made the headline throughout the year. At one end, it made cyber security a household talk point, but at the same time, it poses real threat for industrial and critical infrastructure that hosts lot of aged infrastructure across the industry.

> The cyber security ownership and responsibilities should be established clearly between the IT and the operation's organization, under a common leadership. While IT teams focus on protecting data and systems, their OT counterparts must protect mission critical assets and control systems.

There have been a few other geo-political activities as well that may develop into new risks in future, but overall this year saw India's cyber policy landscape evolving with the Supreme Court's judgement on privacy and data privacy bill roadmap, to name a few.

How technologies like AI can be useful to your industry? In which areas AI can be useful in security?

In past machine operators and technicians monitored engines and machines by listening to their clanks and checking their gauges, but today sensors and machine learning offer the same and much more by providing predictive failures and maintenance capabilities. AI is making industrial operations safer and more reliable while helping to ensure optimal performance at a lower sustainable cost.

AI in cyber security, in general, is evolving and is playing an increasingly important role in cyber analytics, especially user entity and behavior analytics, and identity and privilege access management analytics. Many cyber security leaders are watching this space very closely and are experimenting with putting available solutions to the real world problems.

What would be the top trends of 2018? For the digitization of business, which new technology platforms will be considered in 2018?

In my opinion, top technology trends to keep an eye on, in coming times are additive manufacturing, AI, Machine Learning (ML), edge computing, digital twins, conversational platforms and Blockchain. These technologies hold tremendous potential in transforming the world as we know, and have evolved rapidly in the past couple of years. They are bound to get sharper in 2018.

Our security posture is driven by a defense-in-depth philosophy

RAMCHANDRA HEGDE, Vice President, Global Information Security and IT Compliance, Genpact, in an interaction with EC's Rachana Jha, discusses how Genpact is protecting its digital asset using a defense-in-depth philosophy and how new technologies like Artificial Intelligence can be of great help in curbing digital disasters

Some edited excerpts...

How do you see the present scenario of digitization in your industry?

Digitization presents a huge opportunity; both in terms of helping clients achieve their digital transformation, as well as driving digitization internally. It's hard to find a company today that is not involved in at least some stage of digital transformation. In fact, in a recent study of C-suite and senior management that Genpact conducted with Fortune Knowledge Group, 82 per cent of respondents plan to implement AI-related technologies in the next three years. Achieving enterprise impact from digital transformation is challenging with so many disparate, disconnected technologies in the market. Many companies use "Band-Aid solutions" which often result in multiple serial projects, lengthy development cycles, and sub-optimal results. To gain ROI and meaningful business results from digitization initiatives, it is the key to have an open, modular platform that can easily integrate various technologies.

Is cyber security a big concern for your industry?

Cyber risk presents a multi-faceted challenge. Incidents and breaches, or an inability to demonstrate an appropriate level of security can have significant implications on clients' and customers' perception of organizations, which is especially important in an industry like ours where Genpact is a trusted and reliable partner in running our clients' businesses. This is driven by concerns around third party / supply chain risk, as well as regulatory focus on this area. Aside from external attacks from a variety of threat actors, there is the aspect of insider actions, both malicious and accidental, which can create a risk exposure.

What measures do you to take to mitigate these attacks? What are your strategies to combat such security threats?

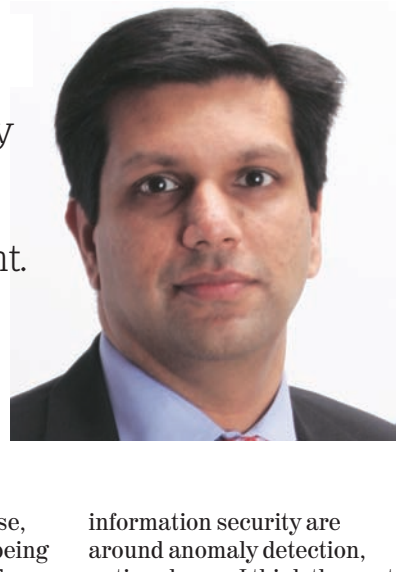
Our security posture is driven by a defense-in-depth philosophy and is focused on the four pillars of people, process, technology, and partnerships. While preventive controls remain very important, enterprises increasingly need to focus on detection and response in today's threat environment. Thus there is a strategic focus on processes and capabilities around situational awareness and threat intelligence and not just incident response, but more broadly around cyber resilience. Also, while more sophisticated technologies get a lot of attention, a relentless focus on basic hygiene is critical as it is the foundational layer.

Today, the insider threat is one important concern for CIOs and CISOs as insiders have more access to information and their activities can go undetected longer than external threats.

What kind of processes do you have in place to prevent unauthorized use of information? What kind of technologies / solutions do you use to prevent theft or leakage of information from insiders?

If the right controls are present, the activities should not go undetected for long, and what might appear to be an insider activity might actually be a manifestation of an external threat. Technologies for access management and Data Loss Prevention have been mainstream in the industry for long, and a key aspect is to ensure these technologies are configured and run effectively. More recently, technologies like Cloud Access Security Brokers (CASB) and User Behaviour Analysis are helping to provide visibility into activities on the cloud, as well in developing as a holistic picture of user activity across multiple systems.

> While preventive controls remain very important, enterprises increasingly need to focus on detection and response in today's threat environment. Thus there is a strategic focus on processes and capabilities around situational awareness and threat intelligence



How technologies like Artificial Intelligence (AI) can be useful to your industry? In which areas do you think AI can be useful in security?

AI holds a lot of promise, and results are actually being seen in some use cases. For example, there are applications in risk management that use natural language processing, machine learning, and other AI technologies to piece together seemingly disparate pieces of information and help companies understand massive amounts of structured and unstructured data in real time. This can help identify and prevent security risks, and also such issues as anti-money laundering, fraud, corporate espionage, etc. While some of the typical use cases in information security are around anomaly detection, anti-malware, I think the next few years will see much broader experimentation and more interesting use cases come out.

For the security analysts, what is the approximate amount of work that will come down by using AI?

It is still early days in this area, and it could well be that the focus and outcome might not be just on the reduction of work, but in a shift in the type of work to more value-added or different work or using AI to augment and not necessarily replace.

Does AI have the potential to segregate false positives from the suspicious traffic?

The potential is already there, especially with the right training sets and process, but again I think it is early days, and there will be learnings from the initial use cases. The system can be tuned depending on the success rates.

Can AI help in pinpointing the kinds of threat vectors which are sitting latent on the network waiting for the right opportunity?

Potentially, there are other controls that can be relevant in these scenarios. For example, isolation platforms, situational awareness and detection technologies also have a big role to play in minimizing the risk exposure. AI will bring great power but will also like require different levels of human intervention / validation and re-architecture of the overall solution framework. Thus, I think a good way of looking at AI is that it will be an important and relevant component of the overall solution framework for mitigating cyber risks.

BSE's Cyber Security Operations Center is AI Enabled

BSE IS implementing a Cyber Security Operations Centre (CSOC) with Artificial Intelligence capabilities on the back of an orchestrated approach wherein multiple advanced cyber technology solutions are integrated to provide contextual intelligence, explains Shivkumar Pandey, CISO, BSE

CSOC AT BSE

- **The** Bombay Stock Exchange (BSE) is the fastest exchange of the world. It facilitates 250-280 million orders per day. Of these about two million trades are converted. BSE has 13 companies under its umbrella. India International Exchange (INX) being the latest entrant, which operates 22 hours of the day.
- **CSOC** will operate 24X7 with a suite of 22 niche and advanced technologies. The solution is also integrated with other intelligent sources that provides alerts about the trending and emerging threat vectors at any given point in time. There are feeds available from CERT-in, IBM, Checkpoint, Microsoft, IDRBT etc
- It a multi million dollar deal with more than 30 per cent of the overall IT budget in 2016-17 allocated for security. There are no licenses bought.
- The solution will take care of the key nine pillars: security of the data, network, endpoint, advanced fraud detection, identity and access management (wherein BSE has taken ARCOS PIM), Open IBM SSO, application security solution, IBM AppScan for source code review and wireless application firewall. For data security: DAM, Network DLP for data classification. For mobile security, a Mobile Data Management (MDM) solution, Mobile threat Management for content security; endpoint patch management, malware protection, endpoint DLP, endpoint detection and response and Network Access Control; feeds for threat intelligence is sourced from various avenues

> In the emerging threat scenario, SOC has limited relevance. The time is ripe for CSOC, which adopts a more proactive response strategy
>
> **Shivkumar Pandey**
> CISO, BSE

Abhishek Raval
abhishek.raval@expressindia.com

The stock exchanges in India, the fastest growing economy are closely watched and reported, globally. The news about any halt or disruption in trade at a stock exchange spreads like wildfire and has tremendous monetary ramifications. The exchanges are seen as a reflection of the health of the economy of a country. The Bombay Stock Exchange (BSE) is the fastest exchange of the world. It facilitates 250-280 million orders per day. Of these about two million trades are converted. BSE has 13 companies under its umbrella. India International Exchange (INX) being the latest entrant, which operates 22 hours of the day. Precisely, why, BSE is a target of cyber hackers and organised cyber crime syndicates. Most of the times, the attacks are state sponsored. This makes cyber security a critical business factor for the BSE. In order to ringfence itself from global cyber security threats, BSE is implementing a next generation Cyber Security Operations Centre (CSOC). "All the 22 tools in the CSOC have been bought and orchestrated together to work as one unit. The CSOC will empower the exchange to have a real time and proactive stance to any impending cyber security threat," says Shivkumar Pandey, CISO, BSE.

The Bombay Stock Exchange (BSE) is in the process of implementing a hybrid Cyber Security Operations Centre (CSOC). "About 80 per cent of the rollout is over, which is scheduled to get in a short period of time," informs Pandey.

Nextgen CSOC: About the implementation

The project timeline is from March 2017 to December 2017. The standard inbuilt configurations are up and running. Some customization based on the existing setup is still pending. This CSOC applies to all the 13 group companies of BSE. It will operate 24X7 with a suite of 22 niche and advanced technologies. The solution is also integrated with other intelligent sources that provides alerts about the trending and emerging threat vectors at any given point in time. There are feeds available from CERT-in, IBM, Checkpoint, Microsoft, IDRBT etc. These feeds are centrally processed and a cyber threat intelligence is generated. This is again integrated with the SIEM and the analytics tool. The solution has been finalised after consolidating various information security frameworks from SEBI, CERT-in, National Institute of Standards and Technology (NIST) and third party consultants. From a certifications perspective, BSE is already ISO 27001 certified and is under the process of getting ISO 22301 certified. The approximate cost as mentioned by Pandey, "It's a multi million dollar deal with more than 30 per cent of the overall IT budget in 2016-17 allocated for security. There are no licenses bought. The entire hardware is owned by BSE."

The implementation has been done using a big bang approach. All the tools in the suite of offerings have been bought. Given that each of the tools have use cases in the stock exchange space. They are integrated to work in complete alignment. The integration will power the single dashboard to send alerts to the respective stakeholders. The threat will be killed at the source level itself.

From reactive to proactive

Any organization fundamentally faces two kinds of threats: Internal and external. As far as internal threat is concerned, the CSOC has a Network Access Control (NAC) tool, compliance tool like IBM BigFix. It makes sure the tools used by the internal employees are compliant with the BSE's InfoSec policy. The tools will run on the BSE network, only when they are set according to the policy. For the external employees, they will have to be registered first, followed by a request sent to the CIO on the kind of IT tools to be accessed. Accordingly, the required access will be provided.

The solution will take care of the key nine pillars: security of the data, network, endpoint, advanced fraud detection, identity and access management (wherein BSE has taken ARCOS PIM), Open IBM SSO, application security solution, IBM AppScan for source code review and wireless application firewall. For data security: DAM, Network DLP for data classification. For mobile security, a Mobile Data Management (MDM) solution, Mobile threat Management for content security; endpoint patch management, malware protection, endpoint DLP, endpoint detection and response and Network Access Control; feeds for threat intelligence is sourced from various avenues.

To put these solutions together, for them to work in cohesion, there is a security analytics and orchestration middleware. It is supported by cognitive security, threat hunting and investigation, user behaviour analysis, incident management and response, threat anomaly detection and vulnerability management. All these solutions are integrated and orchestrated. The tools, which are operating from the cloud are also integrated with the CSOC. For example, BSE has hooked the Office 365 on cloud.

It's important to note, this is a CSOC and not a SOC, which is more reactive in nature. "In the emerging threat scenario, SOC has limited relevance. The time is ripe for CSOC, which adopts a more proactive response strategy. The systems in a CSOC model are more closely knit together with the people and processes vis-a-vis a SOC model," informs Pandey. It has online forensics, ML, Network Behaviour Anomaly Detection (NBAD). This is all Real time, the feeds are consolidated at one place and analysed for various new age threats like anti advanced persistent threat tool, which neutralises the zero day attack. These are signature based attacks. Moreover, threat intelligence, dark web monitoring tools are also provided, which puts the posture on a more proactive footing than reactive.

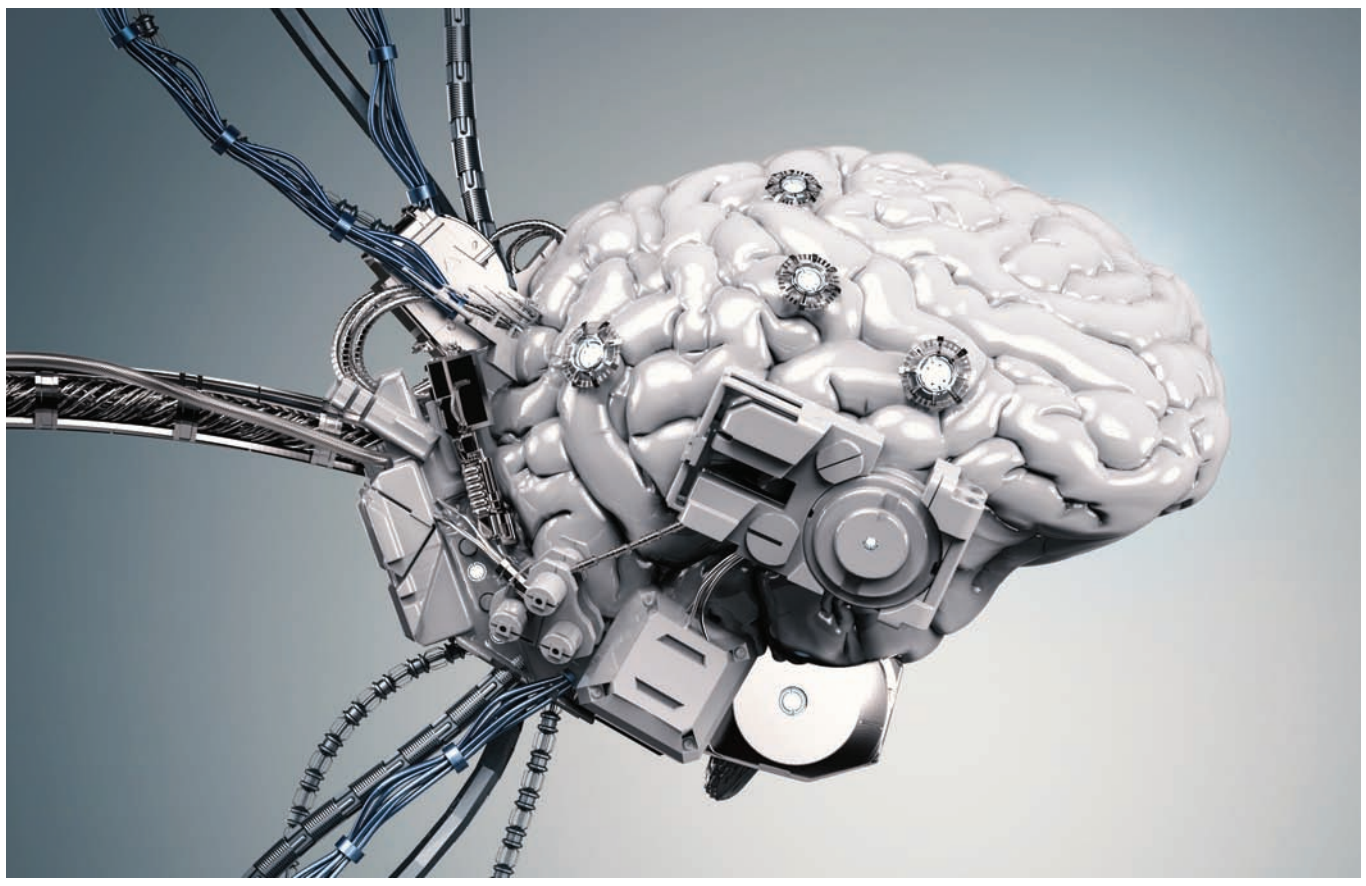
> **We have malware protection tools like Anti APTs, IPS signature based solution and anti virus. We also do simulation tests, to make sure the tools are performing and are up to the mark as claimed and benchmarked by the vendors**

The CSOC runs on a hybrid model. BSE has a captive SOC in Mumbai, manned by 15-20 professionals. In combination, there are 22 security professionals from IBM operating from Bengaluru. There are traditional technologies like PIM, DAM, WAF, SIEM, security analytics etc. On top of this, there are other next generation capabilities like forensics, Anti APT solution, deception technologies etc. The deception tool stops ransomware with lateral movement. A honeypot is created in VLANs, which immediately identifies the scanning and relays alerts from SIEM to the security operations team. The suite of technologies also has IBM watson (with features like ML and predictive analytics). Both the traditional and Next gen security technology tools combine and provide the intelligence to handle not only the scale and size of the systems handled but also events responded to in close to real time and with razor sharp accuracy. The CSOC provides time, scale and accuracy to respond to cyber security incidents. ML adds to the capabilities as far as automation and proactive approach is concerned. The ML learns from both the structured and unstructured data. Using the solution, most of the L1 jobs are automated.

The Bombay Stock Exchange, on a daily basis is under attack from a number of threat vectors. The normal attacks are: DDoS, malware etc. For DDoS, BSE has a hybrid model for security. On premise, the network can withstand 2GB protection. The cloud takes over to face volumetric based attacks. "We have malware protection tools like Anti APTs, IPS signature based solution and anti virus. This apart, we also do simulation tests, to make sure the tools are performing and are up to the mark as claimed and benchmarked by the vendors," says Pandey. The attacks are staged manually from the premises using the red team assessment. For some technologies, these simulation tests are conducted on a quarterly basis and some on an annual basis.

Prakash Arunachalam,
CIO, Servion Global Solutions

Top 8 Artificial Intelligence trends to watch for in 2018



The year 2017 saw both techno stalwarts and start-ups jumping into the AI ecosystem.Suffice to say, Artificial Intelligence will begin to permeate every application and service at some level in the year 2018. According to Gartner, "The year 2018 will mark the beginning of a democratization of AI, extending its impact across a much broader swath of companies and governments than previously". This indicates that AI will be included in the top five investment priorities that CIOs make during the year.

Let us take a glance at what it holds for the customer experience industry.

Go Cloud, Go Smart

AI technologies, especially machine learning and deep learning will emerge rapidly to add more power to the cloud. The amalgamation of cloud computing and machine learning will result in 'the intelligent cloud'. Serving as a self-learning platform, it will be able to perform tasks more accurately and efficiently than ever before. This is likely to be the era of the next-generation cloud, one that provides scalability at a low cost, for storing and processing large volumes of data.

Talking about conversational interfaces

The past year,many vendors have been successful in applying conversational interfaces in smartphones and other devices.Virtual assistants such as Siri, Alexa, and Google Now are already making waves since they cater to the modern demands of the customer through text or voice. Virtual assistants are moving from being purely proactive to being highly personalized. In the coming year, it is expected that nearly 20 per cent of the citizens belonging to developed countries will use AI-powered assistants to help them with various everyday operational tasks and about 40 per cent of customer-facing employees and government workers will consult an AI virtual support agent for decision/process support. The reason being – better collaboration between humans and machines due to improved interfaces and new AI capabilities.

We have to chat it out

The market for bots, especially chatbots, has been gaining a lot of traction.While a chatbot is a stand-alone conversational interface that uses an app, messaging platform, social network or chat solution for its conversations, a bot is a microservice or app that can operate on other bots, apps or services. In 2018, we will see many channel applications adopt self-learning chatbots as a built-in functionality since it goes hand-in-glove with the big boom of Big Data and Analytics while directly reducing direct labour and other operational costs. It will also be a year of blended AI since human interactions will never wane away but they may emerge as the epicentre that drives AI in the customer service industry.

Welcome to the post-app era

Conversational AI platforms will supersede and push the existing paradigm of 'cloud first and mobile first' to the background. These AI platforms will accelerate the growth of AI-related markets. Here is why:

- They move away from fixed commands for communication between people, bots, agents, applications and other services
- Offer a broad range of narrow AI services
- Persists across modalities, devices, contexts while being sensitive to context change
- Makes machines smarter and humans successful in novel situations

This new paradigm shift marks the beginning of a 'post app' era.

Building a new safe zone

As more and more devices get connected, there may arise the challenges of new security breaches. Cyber security experts will need all the help they can to meet these threats. AI systems are designed to detect even the smallest of changes in the environment, and they have the potential to act much faster to fix them. AI will be of tremendous help to identify and analyze such exploits and weaknesses to quickly mitigate more attacks. In 2018, AI-based cyber security technologies will become more mature.

Let's get emotional

In 2018, AI will slowly start to further mould the way we interact with daily technologies. Gartner even boldly predicts that in the coming years, personal devices will know more about our emotional state than our own families. As more and more user data is collected and analyzed to create better contexts, it will be a turning point for users to spend more and more time with devices such as smartphones, wearables, and PC. Emotional AI detects emotions (happiness, surprise, anxiousness, sadness, anger, fear and a neutral state) through voice intonations or facial expressions. This will be added to theeducational software, video games, and diagnostic software to provide a much more personalized experience.

A very deep impact

AI is not restricted to the realm of software alone. Thanks to deep learning, a new name for neural networks may ultimately lead to a hardware revolution. Highly parallel Graphic Processing Unit (GPUs) chips which provide the necessary computational power and hardware designed for Deep Neural Networks will be 100 to 1,000 times powerful than those that are available today. A better hardware architecture has the potential to make a big impact on the next generation of applications. We will see more software companies investing in custom hardware to speed up the processing for deep learning.

Automatic for the people

AI in retail and e-commerce is undoubtedly picking up momentum. As AI begins to become more accurate in its predictions of customer needs, automated purchases that are directly delivered to the customer will become a more compelling option. AI-powered product recommendation engines will target and personalize products that are displayed to the customers. Moreover, machine-learning algorithms will alter recommendations based on the stage or channel a customer is shopping in. With improved logistics, customers too will be convinced and more open to engage with this type of purchase.

While the year 2018 is poised for greater impact of AI, many organizations are still not equipped with the right skills. Technical skills such as deep learning are at a nascent stage. Technology business leaders must understand how to successfully leverage opportunities that AI presents, instead of remaining averse to it as a passing fad. After all, AI is here to stay. The year 2018 will indeed make a stronger case for it.

Ashutosh Jain,
CISO, Axis Bank

Understanding the basics of enterprise security

The cost of security should not only be considered keeping in mind the breach scenario but also the digital roadmap of the organisation. This sheer aspiration of companies to connect with their customers, employees, shareholders and other stakeholders, through digital means brings along with it, an inherent risk of security too. The investments in these digital solutions also brings the cost of security under its realm.

As a natural progression, the question arises on the rationale for investing in security when on a daily basis, there are no major security incidents involved. It's the same reason as to why protection like seat belt and helmet exists. Similarly, there are a plethora of security procedures in various industries like airlines, manufacturing etc. One has to be cognizant of the security risks because when the accidents occur, they come with a sheer sense of surprise, and are unannounced. More importantly, it bangs the company with a reputation loss, which can prove too severe to make any come back. The cyber insurance can surely compensate for the monetary loss but disrepute can be permanent.

The bottomline is information security becomes a part of the business when it is thought about simultaneously with the digital path the company has visualised. Hence, security no longer remains an afterthought.

Challenges for CISOs

In the wake of increasing digitalisation, availability of the required IT security budget is not a challenge for CISOs. The challenge is the lack of understanding in deciding why a particular security tool is useful. Many security professionals lack the skill of recognizing, understanding the problem and then having the right viewpoint to find a solution.

Often, they end up buying a particular product because a company in the same space has bought it. The same applies not only for products but also implementation partners. There is no sound rationale. Just because, a peer has bought a product from a particular vendor; hired services from a specific implementation partner, certain Infosec professionals do the same. A number of these professionals still cannot grasp, what is an Intrusion Prevention System (IPS) and why is it required?. They have a misconception that an IPS is unnecessary, when a firewall is already installed. The truth is, IPS is critical for certain deep packet attacks on the network. One needs to understand how the attacks are carried out, detected, trapped and then remediated. But unfortunately, this understanding is missing in some CISOs. The end result - CISOs land themselves in the tangle of buying products that others are buying. Consequently, and naturally, there is no RoI and as a result, no budgets are allocated for any other solution. It's a vicious cycle.

The bottomline is information security becomes a part of the business when it is thought about simultaneously with the digital path the company has visualised. Hence, security no longer remains an afterthought

CISOs should have an in depth understanding of the security products. Right talent should be hired before building teams with complementary skillsets, who can get to the root of the problem and take the right decision. Budget is not a constraint if these prerequisites are in place. Money will never be a roadblock if the problems are understood in its entirety and a close to foolproof solution plan is proposed.

Security: Not a function, but everybody's job

Security should be inculcated in every practice and function of the IT department. For e.g. developers should understand the importance of secure coding. This helps in managing security right at the root, i.e at the coding level. Understanding the different ways in which the code can be compromised and then looping security, can be a best practice. The network admins can explore secure network architectures. Every function in IT should think from a security angle to whatever they buy, do and implement. As far as budding security professionals are concerned, developing a deep technical domain expertise is a must.

Going forward, threat hunting and modeling professionals will be in demand in the future. While there are many professionals getting into security testing but from a security architecture, threat modeling and cloud security angle, there is not much talent available. These areas require a deep intellect.

CISO reporting structures

The CISO function is becoming equivalent to other CXOs, so much so that in some organizations, the CISO directly reports to the board and not the CEO. This development is in the aftermath of the recent spate of ransomware attacks and also due to the imposing threats that lingers as cybercrime has become more organised. However in the BFSI industry, the CISOs are supposed to report to the respective CXOs as mentioned in the RBI guidelines. It is either to the Executive Director or the Chief Risk Officer. The board members are extremely concerned about cyber security and many direct questions are asked. They do ask the right questions and ask for relevant advice. This is becoming an industry wide phenomena. The members are also pointing to the right directions on managing the security posture. India is much better placed in this respect than many other countries.

Potential of AI in solving security issues

AI and ML has huge scope in solving the information security challenges and there are vendors who are already claiming ML capabilities in their solutions. Even hackers are trying to use AI to stage attacks. The defendants in this case, will have to do catch up. AI has tremendous potential but capturing the data from various nodes is critical. Data can either be captured, processed from one point or at various nodes. Endpoint behaviour analysis tools exists and we use some of them also. There are deep tools, with advanced analytics capabilities that can process data centrally too. AI will have an edge over other tools in segregating the false positives from the suspicious traffic.

V Swaminathan,
Head - Corp Audit & Assurance, Godrej Industries & Associate Companies (GILAC)

Godrej Industries has taken proactive steps in cyber security

Godrej Industries & Associate Companies (GILAC) is a large conglomerate having diverse set of businesses which throw unique challenges at us every day. Each business operates in multiple geographies (including international) and has completely different line of business, level of automation, skill sets and awareness of people. As a result, the security solutions these businesses need are also different. Add to it the already complex landscape of new technologies and related risks which need to be addressed.

Being a part of this complex setup as CISO increases our understanding of existing , new and emerging risks in the IT /security landscape, about latest technologies and related information security requirements. It also pushes us to regularly update ourselves with new developments and innovations which can be used for the benefit of business.

Information Security in GILAC has always been given its due importance. ISO 27001 was implemented in 2008 and full-fledged Information Security function was established. The IT & Infosec Steering Committee chaired by our Chairman meets and reviews the IT and Infosec roadmap, new emerging risks in the technology landscape and approves measures to mitigate such risks.

Risks in our sector

Godrej operates predominantly in the manufacturing sector and has its own set of security challenges.

The manufacturing sector is steadily budging up the list of industries at higher risk of cyber crimes. Hackers are now realizing the attractiveness, value, vulnerability, and sensitivity of the manufacturing sector. This sector is more susceptible to cyber crimes because companies in manufacturing have not fully realized the importance of cyber security yet. They are not fully ready and equipped to cope with an attack.

The manufacturing sector players like FMCGs, locomotive, textile, pharmaceutical, chemical, and defense goods producers hold critical data and information. They conduct researches and developments. They have a cache of patent and IP related information and business secrets. This makes them an attractive niche for cyber criminals. The risks are greater in that, the manufacturers depend mostly on systems and networks that lack robust cyber defenses.

Apart from this, some areas of emerging risks are:

- Cloud computing
- Cyber security
- SCADA system security.
- Bring Your Own Device (BYOD)
- Internet of Things (IOT)

Information Security @ Godrej Industries Ltd & Associate Businesses.

Godrej Group took note of Information security risks and very early on agreed to implement enhanced security measures across the group.

This was almost 8 years ago when even banks, Insurance and technology driven industry were ramping up their security processes.

Every CISO dreams of implementing a fortified system in his organization which is virtually impenetrable and is immune to almost every risk. However, businesses have also to balance the costs of managing such a fortress Security system v/s the demand for a higher level of flexibility and ease of business operation. , sometimes, at the cost of security.

Our Chairman Mr Adi Godrej and all Business Heads have always extended their 100 per cent support in favour of having a good IT Security Infrastructure, even if it means some inconvenience in business processes.

Information Security team's endeavour has always been to explain to the leadership team, Information Security Risks and its implication in the Medium and Long term. The Group has never shied away from investing in efforts to mitigate such risks.

Apart from the top management support, one of the key to the success of the Information Security function in Godrej is the collaboration with the CIO and the entire IT team, without whom the Security process would slow down. The CISO and CIO work together to implement practical and cost effective solutions which helps the organisation mitigate risks.

Apart from the top management support, one of the key to the success of the Information Security function in Godrej is the collaboration with the CIO and the entire IT team without whom the Security process would slow down

Data Leakage Prevention (DLP) & ISO 27001 at Godrej Industries Ltd and Associate Businesses

Godrej group operates in a very competitive business environment, especially our FMCG business where new innovations, product launches, marketing strategies etc. are very sensitive information. Godrej has a significant investment in its R&D initiatives in the FMCG, Agri and Chemical space and information security in these areas are very critical.

The group has made all efforts to protect such information through multiple ways

a) Regular Awareness created amongst employees about the information security policy, sensitivity of data and the need to securely store and share only on need to know basis.
b) Monitoring the flow of sensitive information through a DLP programme
c) Hardware checks and monitoring at sensitive functions.

As mentioned earlier, ISO 27001 was implemented 8 years back. We have a robust process with Business Information Security Offices (BISOs) and Unit Information Security Officers (UISOs) regularly monitor implementation of Information Security Policies and processes.

Ongoing Security Initiatives

Some of the ongoing initiatives are

a) Delinking the SCADA systems from the Internet and completely segregating the SCADA infrastructure. This is extremely critical for some of our Chemical and other automated plants which can be very vulnerable to any external attack.
b) Data Leakage prevention and security data on the mobile computing platforms are priority initiatives as of now. We are addressing this in a very holistic manner through suitable policies, awareness and technology.
c) Internet of Things (IOT) is a major initiative in our FMCG business where Big Data, Predictive Analytics are gaining momentum. Robust Security architecture and monitoring mechanisms are in the process of implementation.

To conclude, organizations are now heavily dependent on Technology solutions to drive business and Information Security requirements are getting challenged all the time

The field in which we CISO's operate is changing at a very fast speed. The Board of Directors of most companies are now demanding full scale updates on the Information & Cyber security practices of their organizations directly from CISO's. CISO's role will be extremely important and would become a catalyst in organizations growth agenda going ahead.

Prashant Dhanodkar,
Chief Information Security Officer, SBI General Insurance

Cyber Security: All stakeholders should work hand in hand

Internet access in today's world has become as routine as it gets. Service providers in present times are making data plans available at a minimal cost, leading to higher digital penetration. India is one of the very few economies to boost of over 100 crore mobile phone users. The Government is also committed to increase the digital footprint in our country through its Digital India programme. All this has led to the emergence of electronic transactions for business, like online banking, online insurance, funds transfer, bill payments, e-wallet payments as well as recreation like online shopping, movie/train/air ticket bookings, with utmost simplicity.

While these transactions have made the entire globe a unified, connected marketplace, a digitized economy runs the risk of being confronted by an inevitable security threat. The responsibility of combating this challenge lies with retail and institutional audience alike. The Banking, Financial Services and Insurance sector, popularly known as BFSI, is particularly exposed to cyber threats, given the nature of transactions involved. Since all the personal information of an individual is aligned on these digital platforms, it is of paramount importance to ensure that the same is not leaked as the ramifications of these could be critical to the trust placed on the organisation.

The BFSI organizations are aggressively dealing with information and cyber security, which is treated as a business issue and deliberated at Board level. The management is fully aware of reputational and opportunity losses which may incur due to data security breaches. Hence the Security Governance measures interwoven with Corporate Governance are being put into place. Business balanced scorecards (BSC) are being tweaked to accommodate security compliance. The work force is being constantly trained on their security responsibilities. Organizations are keenly driving customer awareness campaigns around data security using multiple aids like mailers, advertisements and customer portals etc.

With respect to usage of security technology, BFSI organizations are protecting their 'Crown Jewel - Customer Data' with multi-layered security tools. Apart from conventional technologies like Firewalls, Intrusion Prevention, organizations are rapidly embracing latest tools like Data Leakage Prevention, Data Encryption, Web Application Firewalls, Zero Day attack protection, Mobile Device Management (MDM), Information Rights Management (IRM) Security Incident & Event Manager (SIEM) and Threat Hunting etc. Majority of BFSI have implemented 24x7 alert monitoring by commissioning Security Operations Center (SOC).

The criticality of Information & Cyber Security is recognised at a Government level as well. They are committed to spreading security awareness through the establishment of Cyber Swachhata Kendra (www.cyberswachhatakendra-.gov.in) and CERT-In advisories. This portal provides useful alerts on cyber threats and user friendly tools for removing BOT malwares and protection of mobiles, USB devices and browser security. Most of these tools can be downloaded free of cost. The role of the Government is not limited to the advisories but it is also working on Data Protection Act, which will soon be an integral part of our Constitution. Given the various data repositories that exist in today's times, this Act is being drafted keeping personal information protection in focus. Needless to say, such a law is need of the hour in today's internet driven economy.

The industry regulators like IRDAI, SEBI and RBI are equally committed to ensure security measures and have commensurate guidelines for the same. Many insurance companies including SBI General, banks and NBFC have adopted best security practices in their efforts to secure customer information.

The onus of protecting individuals from cyber security does not rest with the Government and business organizations alone.

Thus, prime importance is being attached to information security by the Government at a Centre and State level, regulators and business organizations. These efforts will, however, only be prolific when an individual is practising safety at their personal level.

DSCI's Annual Cyber Security Summit urges privacy and data protection readiness

OVER 150 SPEAKERS in 60 sessions participated in plenaries, debates, keynotes, visionary talks, in-depth workshops, and roun dtables showcasing security-driven deliberations in this year's summit

Rama Vedashree, CEO, DSCI

Raman Roy, Chairman, NASSCOM

Nasscom's Data Security Council of India (DSCI) recently concluded the 12th edition of its flagship cyber security event, the Annual Information Security Summit (AISS), held in Delhi. AISS is one of the coveted industry summits focused on contemporary and futuristic technologies to address global and national cyber security challenges. This year there was a special focus on privacy, data protection and emerging technologies.

According to DSCI, over 150 speakers in 60 sessions participated in plenaries, debates, keynotes, visionary talks, in-depth workshops, and roundtables showcasing security-driven deliberations. This year's summit was bigger in scale and participation. The major focus of the three-day event revolved around innovation and entrepreneurship, cognitive security, digital payments, capacity building, malware/APTs, product security, DevSecOps, data protection/GDPR, security journalism, forensics etc.

A glimpse of the few interesting sessions included machine learning for cyber security, crypto debate, scope and future of digital forensics, security design thinking, potent and wider cyber attacks, cyber security framework for smart cities, SMBs embracing digital evolution, demystifying cybercrime strategy for corporate and more underscored the discussions at AISS 2017.

Other highlights included 'SEGAMATHON - Security Gamification Hackathon', simulations, demo theater, roast sessions and student zone. DSCI Excellence Awards were hosted to recognize best practices adopted by the industry, exemplary work carried out in the field of security and privacy, and reward visionary leaders. It also conducted DSCI 'Innovation Box' for identifying the 'Most Innovative Security Product of the Year'.

Rama Vedashree, CEO, DSCI said, "DSCI continues to innovate to make AISS an enriching experience for the security leadership and entire ecosystem that spans nascent startups to global leaders, and customers spanning every enterprise vertical and government. This year we are bringing a special focus on strategic and design thinking to the domain of cyber security and deliberations on use cases and innovation agenda."

Speaking at the inaugural ceremony of AISS, Raman Roy, Chairman, NASSCOM said, "This year at AISS, privacy and data protection can't be the only focus, but also other areas too. One is EU GDPR and Industry Readiness and the recent Privacy Judgment. The data protection law will be a reality sooner than later. This is one area where both IT industry and user enterprises have to gear up their readiness to adopt the best practices of privacy, data protection, privacy by design principles and privacy assessments to benchmark themselves. This is one area where DSCI took the lead with its focus on data protection/privacy and its privacy certification. I urge DSCI and the Privacy Leader's Community here to help our industry and user industry to gear up their privacy readiness."

The event also talked about cyber security skills. NASSCOM and DSCI are focused on skills development and curriculum development for few job roles. But skills gap in cyber security, both in industry and academia, is worrying. Industry-Academia collaboration is happening in a very sporadic fashion; and similarly Industry-User Enterprise collaboration to bridge this gap. "As NASSCOM initiates its broader Skills of Future Program, we would put special focus on cyber security," added Raman.

NASSCOM and DSCI, under the leadership of Cyber Security Task Force envisioned a charter – US$ 35 billion, 1000 startups, one million in the workforce by 2025

NASSCOM and DSCI, under the leadership of Cyber Security Task Force envisioned a charter – US$ 35 billion, 1000 startups, one million in the workforce by 2025. To drive this ambitious vision, DSCI wants to make security in India by growing Indian startups and product companies. Another big area in which DSCI is betting big is cyber security services – this is one area, where it is witnessing potential large IT services growing their cyber security portfolio and also niche security services firms like cyber defense centers/cyber fusion centers, SCADA security and advance forensics.

DSCI's objective is to act as a catalyst for startups working in the cyber security space to come up with more innovative product ideas and address real risks, build resilience, increase the trustworthiness and create a conducive environment for businesses. Nine startups were selected for the 'Most Innovative Product of the Year' at the AISS 2017 to provide impetus to budding security product companies. Lucideus Technologies and Security Brigade were announced winners and AppsPicket occupied the runner-up spot at the awards night during AISS 2017. The initiative is an attempt to provide support to product companies in various aspects by bringing these new players nearer to established security leaders, innovators and other stakeholders on a common platform for idea sharing, guidance and collaboration.

INTERVIEW

Aegon Life Insurance aims paradigm shift in healthcare insurance space through IT-enabled approach

AEGON LIFE INSURANCE has performed well on major ratios pertaining to the insurance industry. The persistency ratio, which defines the amount of business retained during the year is close to 95 per cent. The policies sold using the digital medium has jumped to more than 100 per cent in 2017. The claim payout ratio has also improved. **Martijn de Jong**, CDO and VP, Digital – Asia, Aegon Life Insurance, shares about the company's digital initiatives, IT-enabled preventive healthcare, plans for 2018 and more

What are the initiatives taken at Aegon to use digital in cutting the middleman out?

Ease of use is at the center of what Aegon does: Make it as easy as possible to use the website; understand and purchase the product, issue policy etc. Aegon has done website personalisation in the form of Data Management Platform. It has segmented customer data and accordingly the best products are suggested to the customers.

Aegon has built an analytics platform that can hyper-personalise and target the right policy at the right time to the right customer – targeting customers of a certain age/ certain phone model etc. We do a Dynamic Creative Optimisation (DCOS). For example, a customer visiting Facebook and has two siblings will be shown a banner ad having a policy information with a two-sibling scenario. Thus, the offer becomes more personal. Machine Learning (ML) is used for Google Adwords and certain keywords. They are followed in real time and culminated with either bidding higher or lower, based on what is the bounce rate it gets. The higher the bounce rate, the lower the bid.

At times, certain keywords seem to have a high probability for response, but they don't result in expected leads. AI and ML are also used for automatic underwriting and for providing personalized consumer content. Many leads get generated, but not all of them are converted. Leads are nurtured based on the number of mails sent. Subsequently, based on how many mails are read, opened etc, a follow-up action is taken by sending SMSes and calling the customer. Aegon has a venture fund and has invested in an AI company viz. H2O.ai. It's one of the top three companies, globally in the space of automatic underwriting and marketing optimization, which is a dedicated field in AI. By February 2018, we are targeting a surge in 50 per cent conversion rates of the leads, using H2O.ai. The company calculates and recalculates the customer propensity to buy based on the response on mails, SMSes, Facebook, Google etc. An appropriate action is taken accordingly. Significantly, Aegon has a lean analytics team of just five data analysts. In spite of such a small team, they are handling three global analytics projects for Aegon.

Usually, after checking the quote from Aegon, the customer goes on a discovery mode. After the customer comes back on the Aegon site, checking the quotes offered by others, the website immediately pops up the quote, the customer checked before he left the site.

The processes are set such that a policy can be issued in 48 hours. A number of processes are STP enabled. We are able to measure the number of customers leaving the website and then coming back to purchase the policy.

What are the digital initiatives to be taken by Aegon Life in 2018?

Forty eight hours issuance process – for straight-through processing cases it will be immediate issuance – for cases with medicals it will be maximum 48 hours after the medical. Open APIs to partners – eight APIs in total – significantly reducing time to integrate with distribution partners. We are also going to undertake multiple ML/AI projects and pilots including SEM Bid Optimization, Automatic Underwriting and Personalization lead nurturing; alongside personalized web journey including DMP, Data Lake in AWS with ML/AI Datarobot, Blockchain consortium with B3i, new website and user journeys, ARC digital – for certain offline products it will be 12 minutes issuance for straight-through processing cases, large customer driven innovation project, and a number of pilots on preventive health (IoT, wearables, ML/AI) and customized pricing.

Could you share the top five use cases, implemented by realtime digital marketing platform Plumb5?

One is relevant dynamic product banner display: Every new visit on site – Plumb5, displayed the product banner based on the product page viewed by the visitor in previous sessions. For example, if in previous visit, the visitor viewed icancer product pages, in his next visit the homepage banner depicts icancer related banners. The banners were displayed with dynamic quote values (sum insured, premium etc, as per the quote created by lead). Some of the other use cases are automated mails for leads bouncing off; capturing email click as leads for the hot-leads; automated birthday banner, with dynamic delta premium; and automated webpush notification, with dynamic quote values (as per the quote generated by lead).

Could you elaborate on the project on IT-enabled preventive health?

We are running a number of pilots on preventive health and customised pricing. Insurance has traditionally been a reactive industry. It should take a proactive stance, going forward and our preventive health and customised pricing is a step in this direction. Usually, the insurance company-policyholder relationship is where an event happens and the payment is made. Aegon wants to change this paradigm. The objective of the customer is to live long and healthy and our goal is to create an ecosystem around him to make him live a healthy lifestyle. The company is running a pilot on measuring the policy holder's health realtime in partnership with health-tech partners, using wearables and based on the various health related performance metrics the company will reward the policy holder. For example, cheaper gym membership, vouchers, access to health coaches, doctors, do diabetes testing and other rewards are given after completing 10,000 steps or running for a certain distance daily. This is done in accordance with the customer's approval.

We give an ecosystem to the customer to do the sports, measure the health, access to the doctors, sports, health and nutrition coaches. This offering will be attractive to a large number of new customers. India's young population is extremely health conscious. The moot question asked in India to every transaction made, is 'what's in it for me?' and in the case of insurance, it's always not exactly visible, in spite of the policy cover, because the payout only happens after certain events.

Aegon, in partnership with a health-tech partners, is running a pilot of an app for diabetes patients. Aegon is working with an Indian company that owns a health-tech platform. It helps the customer to stay healthy.

Please brief us about the APIs for enhanced service delivery.

Aegon works with a number of partners – brokers, agents, aggregators, health-tech companies, robo advisories. It's important to connect with them fast and transact information. We have developed eight APIs – two of them are live. API enablement helps in turbo charging the information exchange. In the case of one of the aggregators with whom the company works, earlier to the API formation, to enable a particular feature, it took four weeks for the integration and testing. However post the API enablement, we have run 35 test cases in eight hours.

The policy set up, medical appointment, lead setup, lead premium call etc have been automated. These features can significantly boost the engagement level with the customer. The idea is to take the engagement to the next level. Rather than calling the customer every month for asking the premium, it's more apt to touch base with him to check for how would he like to connect with the healthcare ecosystem created by Aegon. Based on the various metrics set by the company, how has the customer performed on the amount of running done/ steps walked, calories burnt etc. Creating a healthcare ecosystem and engaging with the customer is a better relationship than just sending reminders and asking for information. This model of preventive healthcare has worked for Aegon globally. It also helps in customised pricing. IRDA is supposed to clear customized pricing, which lets insurance companies reduce their premium on the basis of health metrics. The customer can earn a low risk premium if the metrics are improving. Some of the European countries are already offering customized pricing.

AI should be introduced much earlier in the insurance lifecycle. It will help in faster policy issuance, at times even without a need to do the medical. AI has prospect in finding proxy data and evaluate whether or not there is a need to do the medical examination of the customer before the policy is issued. In majority of the cases, medical is done, which is time consuming and results in bad customer experience. AI can help in arriving upon a risk score based on certain algorithms run over the proxy data. There are certain correlations which can be established based on the conclusions and inferences. In the US, there is a correlation set between late credit card payments and car accidents. It is said that customers who pay their credit card bills late are more likely to suffer car accidents because of the mentality of the characteristic of late payment will also reflect in driving.

The objective of the company is to issue the policy as soon as it is bought; for which, the medical has to be avoided. Hence AI has to be introduced early in the process. A good risk assessment in the beginning will result in much lesser problems at the end.

Hewlett Packard Enterprise

PRESENTS

Technology Sabha

An Express Group Initiative

INDIA'S LEADING EGOVERNANCE SUMMIT

FEBRUARY 22-24, 2018 | **INDORE MARRIOTT**

PLATINUM PARTNER: DELL EMC | GOLD PARTNER: SAS

LESSONS IN E-GOVERNANCE LEADERSHIP FROM
THE INNOVATORS, CREATORS AND ACCELERATORS

SEEKING E-GOVERNANCE DECISION MAKERS LOOKING TO BUILD PLATFORMS FOR SCALE?

Technology Sabha, has since long been India's premier e-governance forum; setting the pace for e-governance seminars with leadership dialogues, actionable case studies and best practices, networking opportunities and technology showcases.

The 23rd edition of Technology Sabha to be held in **Indore, February 22-24** with the theme **'Lessons in e-governance leadership from the innovators, creators and accelerators'** will gather under one roof the key Government ICT practitioners and decision makers as they work towards the creation of a more transparent and efficient governance mechanism.

WHO WILL ATTEND?

- Secretary & Senior officials from Ministry of Electronics and Information Technology, Govt of India & prominent members from the NeGP
- IT Secretaries from Major States
- e-Governance Heads from State Government
- IT Heads from various Government Nodal Bodies
- IT Heads from various departments of States
- IT Heads from Defence
- IT Heads from Railways

WHY PARTNER

- **Engage** with 100+ key Government decision makers and be a key driver in the new opportunities and spending on ICT solutions, software and technologies in the government
- **Establish** your position as Thought Leader with leading government organisations as they discuss the most critical and current issues in IT that they face.
- **Leverage** the power of a well co-ordinated marketing plan that reaches this august audience through editorial, print, online, eNewsletters and post event coverage.
- **Network** in relaxed, congenial settings with the creme-de-la-creme of Government IT leaders over 3 days.
- **Gain** insight into India's e-development plans along with specific road maps for individual states, helping you to identify and define future business opportunities
- **Enjoy** complete peace of mind knowing the event now in its 23rd Edition is brought to you by Express Computer and the Indian Express Pvt. Ltd.

PARTNERS

PRESENTING PARTNER: Hewlett Packard Enterprise

PLATINUM PARTNER: DELL EMC

GOLD PARTNER: SAS

DIGITAL TRANSFORMATION PARTNER: NUTANIX – Your Enterprise Cloud Platform

PARTNER: AGILE LABS – Making 'IT' really simple

AIRLINE PARTNER: IndiGo

FOR MORE INFORMATION CONTACT

Harit Mohanty (Sales): +91 9821015167, harit.mohanty@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, Navneet Negi – +91 8800523285, navneet.negi@expressindia.com
Mumbai: Shankar Adaviyar – +91 9323998881, shankar.adaviyar@expressindia.com, Nirav Mistry – +91 9586424033, nirav.mistry@expressindia.com
Bangalore / Chennai: Kailash Purohit – +91 9552537922, kailash.purohit@expressindia.com | **Kolkata:** Ajanta Sen Gupta – +91 9831182580, ajanta.sengupta@expressindia.com,
Debnarayan Dutta – +91 9051150480, debnarayan.dutta@expressindia.com
Hyderabad: E Mujahid – +91 9849039936, e.mujahid@expressindia.com, Debnarayan Dutta – +91 9051150480, debnarayan.dutta@expressindia.com

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

spreading out the wings of transformation

Scaling higher with new benchmarks of excellence

Gartner

Sify named a 'Challenger' in Gartner Magic Quadrant 2017 for Managed Hybrid Cloud Hosting – Asia Pacific*.

CIO CHOICE 2018

Data Center Transformation & Network Transformation

Starting the year on a winning note brings a huge wave of inspiration for us at Sify. Something that celebrates our incessant efforts at triggering innovation, and further keeping you ahead with breakthroughs in integrated technology transformation.

Agility | Flexibility | Choices

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

*Gartner, Magic Quadrant for Managed Hybrid Cloud Hosting, Asia/Pacific, To Chee Eng | Kenshi Tazaki | Arup Roy, 31 October 2017
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.