IT NEXT

FOR THE NEXT GENERATION OF CIOs

A DECADE OF
NEXT100

The first batch of
winners reflect
on the award, its
importance, the role
of IT then, now and
in future...

CFO

INDIA

NETWORK

Intelligence . Leadership . Transformation

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

NEXT100 turns 10

> "Awards are supposed to be the culmination but NEXT100 is the start of a journey for most winners"

Shyamanuja Das

Awards—especially those meant for professionals—are primarily celebrations of their achievement, either over a period of time or for a specific job(s) well done. Awards do create expectations for the future; but they are not about the future.

NEXT100 is an award that is essentially about the future. Its positioning quite explicitly states that. For the community, the value is in getting access to a set of next generation leaders—not two or three or even 10-20, but a hundred of them—year after year. It is essentially about creating a pipeline.
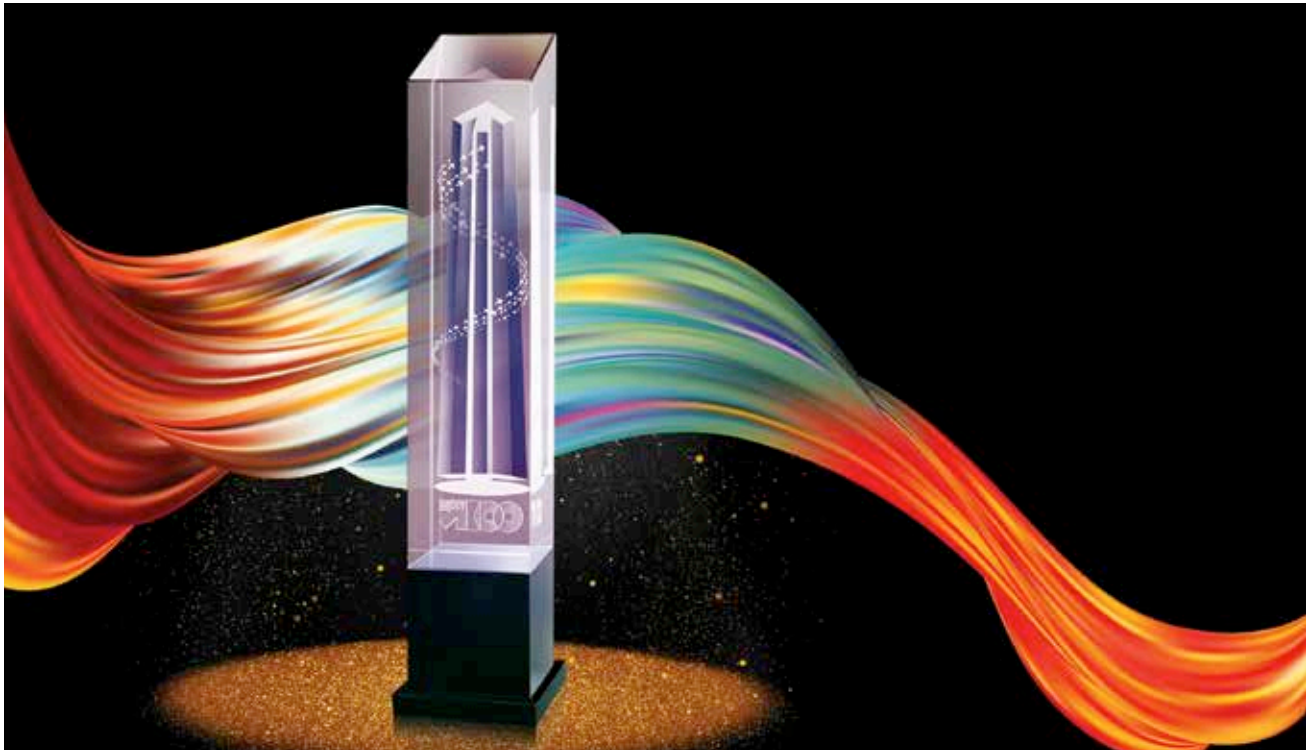
Yet, it is also about celebrating, when that celebration actually matters a lot. We have so many community awards conferred on CIOs and CISOs; even, we have had a couple of such awards in the past. They may have been decided in a very fair and transparent manner. But they are just another set of awards for the recipients. In contrast, the NEXT100 awards are….well, why don't you ask a winner directly?

Some such winners—from our first batch—tell you what the journey has been; the change that NEXT100 has made to their careers and what they plan to do next. This, even as we get ready to hand over the tenth set of awards.

We have always thanked the participants for their enthusiastic response to the award—applying, taking tests, being interviewed. We have also thanked the jury members for their selfless services; they neither get money or recognition for their time and energy; yet, they have been doing it for the community, year after year. We have thanked the sponsors who bear the cost and make it possible.

I will take this opportunity to thank another set of people who have transformed NEXT100 awards from just another set of awards to what it is today. It is those organizations that have looked for NEXT100 awards in the CV of applicants for their senior IT positions. It is those organizations that have made NEXT100 a necessary condition/catalyst for promotion within their IT departments. It is those CIOs who have gone out of their way to encourage their juniors to participate in NEXT100. It is those organizations and individuals who I would like to thank profusely at this point■

Content

A DECADE OF NEXT100

The first batch of winners reflect on the award, its importance, the role of IT then, now and in future...

Cover Design:
SHOKEEN SAIFI

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

EXTRA Curricular

Musings of an inveterate traveller

Travel Along

NEXT100 Winner 2018 **Aditya Khullar**, Technical Leader India - Cyber Security, Paytm shares his passion for travelling and his advice for young travellers...

"I travel not to go anywhere, but to go. I travel for travel's sake."
– Robert Louis Stevenson

"Travelling is not something you're good at. It's something you do, like breathing." – **Gayle Foreman**

"Travel...the best way to be lost and found at the same time."
– Brenna Smith

"Man cannot discover new oceans unless he has the courage to lose sight of the shore." – **Andre Gide**

Travelling is a spiritual experience. It helps see contrast, and appreciate the contrast. You learn that you are a speck in nature, and probably inconsequential. You learn that the life you live is not the only way to live. There are so many people with so many situations, seeking so many things. That, there are many ways to live and be happy.

There is peace in knowing that what you see, feel and experience is not permanent. Travelling often brings one to the point where one seeks peace and joy with their loved ones. You remem-

Aditya Khullar

Aditya Khullar is NEXT100 Winner 2018. He is Technical Leader India - Cyber Security at Paytm. He has worked in companies like Interglobe Enterprises, CB Richard Ellis (South Asia) and BA Continuum India.

He has done both his Masters and Bachelors in Engineering & Technology. He is also Cisco Certified Security Professional (CCSP) and Cisco Certified Internetwork Expert (CCIE).

ber how to use your instinct. Talking to locals in other towns, cities and countries helps develop a sense of empathy to what others are seeking for in life, and relate to things we might normally never relate to. You also get a sense on how cultures have evolved and relate to one another. You learn that as everyone's goal is different on the planet, what we all as human beings seek is – Acceptance, Security & Love. Basically it opens your mind and heart. Spending time and money on experiences is hence a million times better than spending them on materialistic belongings.

My father was an avid traveller. When I was young, he used to travel to various geographic locations around the world because of professional commitments. Being a veteran in the tyre industry and having worked for German giants like Good year, Continental, etc., his travel was often to places in Deutschland like Munich, Bonn, Frankfurt, etc.

Seeing him, I always wanted to be like him as kids usually idolize their parents but in my case it was his travel and the travel bag which brought back a lot of goodies!

I have travelled almost half of the world. The first time I stepped out of home was after my Bachelor's degree in Engineering. I was 22 and applied for a MS Course in the US. I got admission in the University of

On a spiritual quest

Texas in Austin and that was the first time I travelled and stayed away from my family. I was scared but looked up to move forward.

Here are some of the snippets of my travels over the past few years:

- 2007 - Travelled to the US for Masters in Engineering program. (Travelled whole of West and East Coast of the US)
- 2010 - Dubai (My father used to work there in Al Rostamani Group as CEO)
- 2011 - Malaysia, Singapore and Bali (After Marriage - Honeymoon)
- 2012 - 2015 - Abu Dhabi, Beijing, Northern India (Shimla, Chandigarh, Nainital, Punjab) and Goa
- 2016 - Toronto
- 2017 - Hongkong
- 2018 - Thailand

Whenever I travel, I convert myself into a localite. One can best enjoy a place, by going and experiencing things which are close to nature and local people.

Hence, my advice to young travellers would be, "Don't live by the guidebook". Guidebooks are useful for a general overview of a destination, but you'll never find the latest off-thebeat path attractions, bars or restaurants in them. For the best stuff, connect with locals to find out what is hot right now■

As told to Dipanjan Mitra, Team ITNEXT

A DECADE OF
NEXT100

The first batch of winners reflect on the award, its importance, the role of IT then, now and in future...

By **Dipanjan Mitra**

"IF THERE'S A BOOK THAT YOU WANT TO READ, BUT IT HASN'T BEEN WRITTEN YET, THEN YOU MUST WRITE IT"

- Toni Morrison

About ten years back, our continuous interaction with the CIO community, which was just about coming to its own, convinced us that what it badly needed was a pool of capable people from the next generation who could be trained, nurtured and entrusted with carrying on the responsibility. Not only was it needed for a smooth succession planning—which, by the way, was not an explicit agenda item for many then—but for building a vibrant, sizeable community that could attract good talent. If you remember, those were the heydays of offshoring to India and every young man or woman who had some degree or diploma in IT was dreaming of joining an IT services company to go and work on projects across the globe. Enterprise IT—let alone being comparable as an opportunity to outsourcing industry—was not even on their radar.

What if a platform could celebrate success of young achievers as well as identify the potential future leaders to create a pipeline of future CIOs? The best next step of a dream is to realize that.

NEXT100 was born. The first set of awards was given in 2010.

It is different from most other awards because:

- It is targeted at next generation leaders. Identifying them was the real contribution to the community.
- It is a transparent, rigorous process with no involvement of 9.9 management or editors in the decision.

The awards are given on the basis of not just their past work, but also their potential, measured by internationally renowned psychometric tests and more importantly actual interviews by top CIOs. It is for, of, and by the community.

The fact that so many of NEXT100 winners today are CIOs and CISOs and many more are on the verge of taking up the big role, convinces us that the time, energy and money that we put in—with active contribution of the CIO community and our partners—has not been wasted. What encourages us even today is that while there are so many awards that are being given these days, NEXT100 winners acknowledge the contribution that NEXT100 awards has done to their careers.

As we prepare for the tenth set of NEXT100 awards, we thought of speaking to the first batch of winners to figure out how the awards mattered to them. All 2010 NEXT100 winners we spoke to felt winning the award has helped their career in a big way. It has helped them professionally to go to the next level. Most of them felt it is a good platform to connect with industry experts and peers from other organizations, which helps in learning and gaining useful insights.

We also got their views on how IT has changed all these years, along with their personal and professional plans for 2019. Here is what we found:

- Most of them felt enterprise IT has evolved from a support function to a business function between then and now. It has become an enabler in business.

- IT now is more independent having its own budget and ability to take separate decisions with regards to buying IT equipments. It doesn't solely rely on business budgets anymore.

- IT functions were mostly done in-house 9-10 years back whereas it has a more customer-centric outlook now. The focus now is to have a better user-experience.

- There was less automation in 2010 and the thrust was on immediate needs. IT has taken a more futuristic approach now.

- Most of the NEXT100 winners also highlighted that they are continuously aiming to upgrade their skills so that they can successfully achieve their professional goals in 2019 and beyond■

AJAY VERNEKAR

Then: VP – IT, Standard Life

Now: CTO, Aditya Birla Sun Life Insurance Co

Role of NEXT100: The application process of NEXT100 was very good. Being part of NEXT100 group enabled me to get into the CIO group for the first time.

Role of Enterprise IT then: There was gap between IT and business.

Role of Enterprise IT now: The boundaries between IT and business have minimized. IT personnel now talk more on business lines.

Professionals Goals for 2019: I want to pursue digital initiatives and achieve exponential growth in my organization.

Personal Goals for 2019: I want to bring in the new tech platform so that we can master AI, Automation, etc., in my organization.

ANAND BUDHOLIA

Then: Additional VP – IT, Reliance Infrastructure

Now: Sr. VP, CIO & CISO, Reliance Power

Role of NEXT100: Winning the NEXT100 award has been wonderful for me. It has had a positive impact on my career and motivated me to work harder for my organization.

Role of Enterprise IT then: Enteprise IT was then in 'partner' mode, having evolved from 'support function'.

Role of Enterprise IT now: Enteprise IT now is more of an 'enabler' in business, having evolved from 'partner' mode.

Professionals Goals for 2019: I want to implement predictive analytics using AI, Machine Learning and IoT in my organization. Right now, everything is at evolving stage. So the challenge is to deploy this at the earliest.

Personal Goals for 2019: Achieving my professional goals is itself my personal goal.

ASHISH CHAKRABORTY

Then: Associate Director – IT, Mindtree

Now: Head – IT & Security, Harbinger Group

Role of NEXT100: Winning the NEXT100 has enabled me to go the next level in my career. Now, I'm basically performing the role of a CIO in my organization.

Role of Enterprise IT then: Enteprise IT had no link with business then. Everything existed in silos.

Role of Enterprise IT now: Enteprise IT now is more aligned with business objectives. This is more in line with the emerging enterprise tech

Professionals Goals for 2019: I want to fulfil my 5 KRAs this year:
- Align myself with the business objectives of the organization
- Implement cybersecurity initiatives
- Implement data privacy and security plans
- Achieve process automation
- Enhance user experience

Personal Goals for 2019: My key aim this year is to be a cloud architect.

BALAJI ALAPILLA

Then: Program Manager, IBM

Now: Associate General Manager, HCL

Role of NEXT100: The recognition has helped a lot in terms of building confidence and connecting with the industry to understand the current trends. It has also helped me to move ahead in my career to the next level.

Role of Enterprise IT then: IT was seen more of a cost for the business.

Role of Enterprise IT now: IT has now transformed from a 'cost' model to a 'business' model. There has been a massive paradigm shift in the sense that these days, business defines IT.

Professionals Goals for 2019: I want to achieve an executive level at my organization.

Personal Goals for 2019: I want to apply my enterprise-level skills and learning to other areas of work in society.

DEBASISH CHATTERJEE

Then: Program Manager, Philips Healthcare

Now: Director - Software Engineering, Philips Healthcare

Role of NEXT100: I felt very happy winning the award although it didn't really impact my career.

Role of Enterprise IT then: IT was more in-house and SAP implementations were in place and had nothing to do with customers as such.

Role of Enterprise IT now: Currently, we are working on medical technologies and applications that directly go to customers.

Professionals Goals for 2019: I want to work towards enhancing my organization's business profitability and market share.

Personal Goals for 2019: My personal goal is to work towards achieving my professional goal.

JATINDER AGGARWAL

Then: Group Manager, HCL Technologies

Now: Sr. VP - Corporate & Investment Banking, JPMorgan Chase

Role of NEXT100: It gave me temporary recognition within my peer group and social media. It also looked good on my resume.

Role of Enterprise IT then: IT was just supporting the business and we were exploring how IT can be taken to the next level.

Role of Enterprise IT now: We are looking at automation and digitalization. Blockchain, IoT and Machine Learning are the main focus areas and we are interested to see how it will change the way business works. So, IT has gone much beyond the consulting function. It's more automated and humans are now competing with machines.

Professionals Goals for 2019: I want to become an entrepreneur.

Personal Goals for 2019: I read a lot and think about new ideas and products and the way future technologies can be used. This will help me to achieve my entrepreneurial dream.

JOSE DANIEL

Then: Head – Operations, Fibre-2Fashion

Now: Executive Director, Fibre-2Fashion

Role of NEXT100: It was an overwhelming feeling to win among so many applicants. It was a positive platform whereby I could connect with various industry people.

Role of Enterprise IT then: There was less automation and the overall spend on IT was minimal. The IT revolution was just starting to take place at that time.

Role of Enterprise IT now: Today, there is AI, ML, IoT, Automation, etc. It is more futuristic and is basically a part of life.

Professionals Goals for 2019: I want to take my organization to a 500 cr value level.

Personal Goals for 2019: I want to take up more social initiatives and activities and give maximum back to society.

OMESH KHANNA

Then: IT Manager, Verint Systems India

Now: CIO, Allianz Worldwide Partners

Role of NEXT100: It helped me in my application to become a CIO.

Role of Enterprise IT then: IT was solely dependent on business. The entire budget was not in IT hands.

Role of Enterprise IT now: IT has now got its own budget. It has now got its own profit center. Organizations can now purchase their own IT equipments too.

Professionals Goals for 2019: I want to become the CIO of a larger organization.

Personal Goals for 2019: I want to upgrade my skills and create new opportunities. Further, I want to work towards achieving my professional dream.

PRAVITHA VIJAYKUMAR

Then: Business Analyst, Dell International Services

Now: Project & Program Manager, Dell International Services

Role of NEXT100: I felt really elated on winning the NEXT100 award. It helped me in getting into Dell, as I was at a transition point in my career.

Role of Enterprise IT then: The urge then was to get all in-house (paper-based) activities automated and reduce the cycle time.

Role of Enterprise IT now: The focus is now not only to reduce the cycle time but to get a quality product out. The focus is more to go on to agile methodologies and intelligence in order to get quick insights and output. Also, now, it's more about getting the development and testing cycles automated.

Professionals Goals for 2019: As IT is moving more towards automation, my goal is to look into other domains, for instance, move from product lifecycle to supply chain. Basically, I want to go up the ladder in my organization.

Personal Goals for 2019: I want to continue with my psychology studies.

RAMESH KESAVAN

Then: Senior Manager - IT, Lear Corporation

Now: Director - IT, Lear Corporation

Role of NEXT100: I felt valued by such recognition. It boosted my morale and career advancement.

Role of Enterprise IT then: The business volume was very less and the impact of IT was minimal.

Role of Enterprise IT now: IT has had a massive impact on boosting the volume of business now to almost 4 times than that of 2010. Now, the team strength has increased, number of systems has gone up along with challenges like application, implementation and integration.

Professionals Goals for 2019: I want to continue working on the enterprise business model. Also, the entire world is moving to automation. So I want to optimize resources and reduce costs with regard to the same, and achieve our automation targets.

Personal Goals for 2019: I want to upgrade my skills so that it can help me move further in life.

Data Lakes: Steering Through The Deluge Of Data

In order to succeed and maintain a competitive edge, organizations are using data – both historical and real-time – for deep learning and analytics

By Deepak Visweswaraiah

Businesses across the world are collecting massive amounts of data on a daily basis from different kinds of data sources, including telemetry and IoT devices, consumer and business data and even social media. As data becomes increasingly integrated into the way we run our lives and businesses, it is extremely critical how enterprises handle the rapid data

growth and manage diverse data to extract maximum business value and to come up with solutions that have real-life implications.

In order to succeed and maintain a competitive edge, organizations are using these data – both historical and real-time – for deep learning and analytics. The insights can be used for improving utilization of resources, cost optimization, one-to-one marketing, promotions and developing new product ideas.

Data lakes: The most important data management infrastructures of tomorrow

Data lakes bring data from different sources under one umbrella, and since it stores both raw and processed data, it helps support various analytics and ML use cases

A data lake is a repository of structured and unstructured data that enables one to derive insights for their business. One can experiment, explore, and iterate very quickly to build use cases and models on the data lake platform. Data lakes bring data from different data sources together under one umbrella, and since it stores both raw and processed data, it helps support various analytics and Machine Learning (ML) use cases.

Data lakes thus today have emerged as one of the most important data management infrastructures and are being adopted widely across the industry. The basic requirement for a data lake is to allow real-time ingestion and historical data storage. This allows the data to be accessible to data scientists through analytics and deep learning mechanisms. Data lakes also have to layout the real-time and historical data in the right data format so that it can be easily and quickly accessed by the user for analytics, aggregation and time-series queries.

For example, cloud-based services could provide predictive analytics and proactive support to optimize operations across the customer's hybrid cloud. This is achieved by collecting billions of data points from the many telemetry services. These data points are stored in a huge data lake – whether they are on premises in a local datacenter or on the cloud. Deep learning algorithms are then executed on this data lake right in the cloud.

Deep learning framework

Data scientists and engineers analyze the data using the latest ML and AI techniques. This analysis offers the most robust, actionable intelligence, and data is presented in ways that enables businesses to make smart and fast decisions.

The platform provides a framework where developers can build and test data science and ML algorithms quickly in the data lake. To run the

deep learning algorithms, a huge amount of computing power is required. Since on-demand compute can easily be bought in the cloud, the hybrid cloud deep learning algorithm can be executed in the cloud too. Once the algorithms are well tested, the data can be moved from or to the data lake to a cloud-based data storage solution.

This solution lets you use multiple industry-leading clouds (hyperscalers like Amazon, Azure and Google) and maintain complete control over your data on dedicated storage systems from such a data solution.

The hyperscaler clouds are used to deploy micro services that compute or act on the data and make results available to applications or users through the Application Program Interface (API).

Businesses often use such analysis for identifying trends and forecasting and to enhance the efficiency of their infrastructure. It can also help in avoiding or navigating future problems by alerting businesses of similar issues from the past.

The introduction of the data lake platform has led to the democratization of data through self-service analytics and has enabled users to explore data more freely.

Data from other curated data sources can be blended with newly explored data in the data lake for advanced analytics and visualizations. Data lakes have enabled agility for the delivery of innovative solutions at several enterprises such as our own. Users can quickly deliver solutions, get feedback, and iteratively refine the solution before production deployment.

Data lakes can provide invaluable insights through a variety and volume of data, including technologies, such as SPARK, SPARK ML Lib, R, Python, Scala and Akka to enable development, deployment, and execution of ML algorithms.

They can contain valuable insights from customer environments, such as workloads, risk prediction

Cost optimization of data lake cluster can be achieved by segregating it into data ingestion (ingestion cluster) which is compute-intensive and data consumption (analytics cluster) which is storage-intensive and on-demand compute-intensive

and utilization. This data can be used for understanding customer consumption patterns and uptake of new features and technologies in the field. It can be further used for data driven product feature deprecation and bug impact assessments in field. These analytics also enable to identify the staff to be trained for new features and counter the everyday challenges in the field.

The cost of data lakes & RoI

With the volume of data growing day by day, the question of data lake sustainability arises simultaneously. Data lake expansion comes at a huge cost; to keep even two years' historical data, one would need a very big Hadoop cluster. And

businesses will not want to get rid of all the historical goldmine data which is allowing deep learning and data analytics that support their data economics vision.

There are, however, ways to cut some costs around data lake expansion. Data lakes costs involve three major cost components: Storage cost, compute cost and license cost. It needs decoupling of the processing framework from the data storage framework which can be achieved by moving to Spark on Shared Files Systems —Spark as computing framework and Shared Files Systems for storage.

Cost optimization of data lake cluster can be achieved by segregating it into data ingestion (ingestion cluster) which is compute-intensive and data consumption (analytics cluster) which is storage-intensive and on-demand compute-intensive.

Data ingestion cluster can be developed based on event-based architecture using Spark, Kafka and Shared Files Systems without using Hadoop. Data analytics cluster needs to follow best practices for data organization. Parquet columnar storage can be used to reduce storage requirement, and it can also enable fast execution of analytics queries.

In fact, it is possible to reduce the number of Hadoop nodes of the ingestion cluster by around 60% by moving the ingestion pipeline from batch processing to event-based processing using various tools.

With data lakes, new business insights and data use cases which were previously considered unfeasible, are now achievable. Companies can now obtain a complete view of their customers, extend the life of their enterprise data warehouse, or achieve a new level of operational intelligence. It not only helps companies to exploit the potential of different data types but also makes legacy systems more efficient by offloading capacity to the newer, more flexible infrastructure■

The author is Senior Vice President, Quality and Manageability Group (QMG) and Managing Director, NetApp India

Synergized Business Continuity Harnessing Software-Defined Resilience

Organizations are creating software-defined resiliency strategies spanning hybrid cloud environments

By PM Dutta

n the realm of cyber-intrusion onto virtual reality, growing corporates are stringently concerned on seamless business continuity. Off late IT is augmented as a service in a delicate dilemma of making a precise and competent decision to avoid degenerative effects on lifeline IT systems and processes in the reality landscape – synergizing to vital lifeline of the organization.

Cyber threat perception is surmounting beyond anticipation, including the growth of sophisticated stealth attacks – with symptotic signatures. Corporates, of late, are moving from a traditional recovery paradigm to an automated and software-defined resilient take.

With increasing cloud-based applications with synthetic traffic patterns, it's an opportune time to move into an agile and flexible network infrastructure. Today, software-defined resiliency approach has become the new buzzword to support the always-on demand from business perspective – a shift of paradigm seems inevitable. Organizations are creating software-defined resiliency strategies spanning hybrid cloud environments.

SDN in a Hybrid Model

Doubtlessly hybrid cloud environment is the most preferable cloud platform with some of the predictions in the cloud market showing that the global hybrid cloud market will grow at 22.5% CAGR (compounded annual growth rate) from USD 33.28 billion in 2016 to USD 91.74 billion by 2021 (a phenomenal growth of 2.76 times !!! in the coming three years).

In this advent of high paced growth, hybrid cloud capable network on SDN would not work, Furthermore with the advent of Internet-of-Things (IoT) and big data, a more robust network is the need of the hour. Organizations today look out for business that will thrust the growth engine for their organization.

Network Scalability

- Promises agility so that new applications and innovations can be designed and deployed
- Enables migration and modernization of application/s in a hybrid cloud environment
- Improves visibility and governance across hybrid cloud networks
- Boosts security posture of the network, data and applications
- Replaces complexity and risk with

Hybrid cloud environment is the most preferable cloud platform with some predictions in the cloud market showing that the global hybrid cloud market will grow at 22.5% CAGR

operational efficiency

In a nutshell, SDN is the answer to all of them. SDN market is expected to grow at a CAGR of 53.9% from 2014 to 2020 to reach USD 12.5 billion at the end of the forecast period.

Some of the benefits of SDN need to be critically analyzed in cognizance to harnessing procedures. SDN-enabled automation improves the security walls of a network as it allows more granular, zero-trust network security. When an organization migrates or upscales an app in a hybrid cloud environment, the SDN across the datacenter network environment gives the programmability to automatically spin up the network resources in line with the workload needs. At the same time, SDN can align network functions instantly to match application requirements while deploying workloads and network functions together.

A Leap to SDN

- To develop software-defined resiliency approach

- To zero in on best SDN technology for eliminating redundancies and improving scalability
- To drive operational efficiency
- To make security walls more robust and scalable
- To transform existing network infrastructures and maximize the benefits of a software-defined environment■

The author is Senior Manager - IT, Balmer Lawrie & Co

The Role Of IT In India's Economic March Forward

The IT industry has grown in revenue to almost 100 times in last two decades from USD 1 bn to USD 130 bn

By Pankaj Gupta

ndia has recently celebrated its 70th Republic Day. This celebration was very special as we recently became the 6th largest economy of the world with the UK just a notch above. We are today confident that India will become the 5th largest economy soon. Going ahead of the UK is really special as it shows India's emerging power. There might be multiple reasons for it but IT and ITeS industry has clearly ensured India's transformation from an agrarian to a services economy, repositioning the country as a knowledge hub, and boosting economic growth.

At the time of Independence, India was an agrarian country and was reliant on import of almost everything from western nations barring food grains. Though we had good production but rain dependency as a source of irrigation gave an erratic pattern to production due to continuous droughts or floods. Due to this reason, our economy was never stable and the nation was entirely dependent on the rain. Other issues were low per capita income, poor iinfrastructure, illiteracy, low development of industries, depreciated economy, unemployment, income disparity, low living standards, underutilized natural resources, high

population pressure and absence of enterprise and initiative. India was a nation beset with problems and it was difficult for anyone to control so many issues spread across like plague.

India's journey has been divided into two major phases, that is, pre-liberalization (1947–1991) and post-liberalization (1991 onwards). Pre-liberalization era can be further divided into three phases. India got the first push to make strong industrial base (1951–65) to construct various industries like iron and steel, heavy engineering and machine building. Most of these industries were state-sponsored and took India's growth to a range of 5–9% during that period and also provided lots of employment, reduced import dependence and enabled some export resulting in narrowing capital deficit. In the second phase (1965–80), India has seen lots of deceleration and decline as there was substantial industrial growth during this period. India saw a growth rate of 4.1% to negative 1.6% during the period. Basic industries that grew were ferrous metal, construction material and mechanical engineering industries, etc. This phase witnessed 1965 and 1971 wars, successive droughts and oil crisis of 1973. All these factors contributed to a very slow and dull phase of India's growth. In the third phase (1981–91), there was industrial recovery and growth was accelerated barring a few setbacks. During this period, major growth happened in chemicals, petrochemicals and allied industries.

The collapse of the Soviet Union and Gulf War caused a major spike in oil prices resulting in major crisis in India and the country was on the verge of loan default and that had to ask for bailout loan from IMF, which demanded deregulation and that made the way to the post-liberalization phase (1991 onwards), and since then India has not looked back. The reforms brought significant upturn trend.

Though India got some export in the IT industry before 1991 but the major change has come post that. The first software export zone which was known

Due to liberalization in the 90s and increased internet usage, India's growth continued at around 6% and the IT sector started growing exponentially

as SEEPZ was established in 1973 and witnessed around 80% of India's IT export during early days. In late 80s and early 90s various US-based companies started to outsource their work on low cost and skilled talent pool in India and today we have more than 10 million workforce in the Indian IT sector. Due to liberalization in the 90s and increased internet usage, India's growth continued at around 6% and the IT sector started growing exponentially. This brought various investments in India to build R&D centers and improved infrastructure to make India a product development hub by 2000. Another significant boost it got was due to Y2K and dot-com boom which provided Indian firms to grow faster.

In 1998, IT contributed a mere

1.2% to GDP but this has increased to around 8% in 2015. Though it does not sound to be more in percentage but in absolute term, the IT industry has grown in revenue to almost 100 times in last two decades from USD 1 bn to USD 130 bn. Earlier, the outsourcing to India was around 25% and 75% on-site; now this mix has changed to 80% in India and 20% on-site. Apart from this, productivity of the resources measured by average revenue per employee has grown from USD 7K in mid-90s to USD 38K in 2014 as reported by NASSCOM. As per NASS-COM, the IT-ITeS industry will account for 10% of India's GDP by 2020, almost a fifth of its exports and about 30 million direct and indirect jobs.

This productivity shift and more jobs have brought high salary ranges and more spending power helping the entire economy to benefit from it. Earlier, IT sectors grew in Bangalore and Hyderabad. Now slowly it has moved to other tier 2 and 3 cities and is bringing major change in India's inclusive growth.

Though India has a great success story in IT and ITeS industry, however, it still needs to do a lot in high-end SDLC processes like high level design and architectural design. Although some of the IT players are building this competency to take up and successfully complete high level jobs, still we, as a whole industry, need to do much to achieve significant milestone in this category. The other area to watch out for is to get competitive edge against countries like China and Philippines.

India has achieved significantly in this area and cast a great success story; however, it still needs to do a lot to tap the full potential. It also needs to be cautious in areas which may potentially be challenged by upcoming/shifting technology and other countries. In order to retain its current dominance in the long run, it needs to be adaptable in this continuously changing environment■

The author is Global IT Director at The Boston Consulting Group

Maximize Your Security Operations Center Efficiency With Incident Response Orchestration

Orchestration and automation can free overwhelmed analysts in the SOC and significantly improve cyber resiliency throughout the enterprise

By Dan Carlson

ts 5:48 a.m. — only 48 minutes into your 12-hour shift in the security operations center (SOC), and you've already investigated three threats. You were prepared for a long shift, but since an analyst on the night crew just quit, now you're covering her shift, too. How is anyone supposed to stay vigilant in the thick of a monotonous 24-hour slog in the SOC?

When you first started, you tried talking to your boss about how incident response orchestration software and other tools

might work more efficiently. Today, you're just trying to survive. It's hard to not feel completely numb when you're buried in hundreds of alerts you can't possibly review.

When the tools in the SOC don't integrate seamlessly into a unified security immune system of solutions, analysts can't make the most of their time. Given the widening cybersecurity skills gap, the rising cost of a data breach and the blinding speed at which alerts pile up in security information and event management (SIEM) logs, security leaders must empower their analysts to maximize their efficiency.

The first step is to give them the tools they need to accurate prioritize all those alerts — but what does intelligent incident response look like in practice, and how can orchestration and automation help transform a reactive response system into a proactive security powerhouse? Let's zoom in on what's holding SOCs back and how an integrated ecosystem of tools can help analysts overcome these challenges before, during and after an attack.

Learn to Orchestrate Incident Response
■ Reactive, Manual Processes in the Understaffed SOC
The average security analyst investigates 20–25 incidents each day. It takes the average analyst 13–18 minutes to compare indicators of compromise (IoC) to logs, threat intelligence feeds and external intelligence, and manual research can yield false positive rates of 70% or higher.

To make matters worse, as security analysts struggle against an increased volume of complex alerts, the SOC is facing a talent crisis: 66% of cybersecurity professionals believe there are too few qualified analysts to handle alert volume in the SOC.

According to the Ponemon Institute's "2018 Cost of a Data Breach Study," the average cost of a breach globally is USD 3.86 million, a

6.4% increase from 2017. As threat actors become more effective at evading and targeting the enterprise, the majority of analysts can't keep up. 27% of SOCs receive more than 1 million alerts each day, and the most common response to alert fatigue is to modify policies for fewer alerts.

Orchestration and automation can free overwhelmed analysts in the SOC and significantly improve cyber resiliency throughout the enterprise. In fact, research has shown that SOC orchestration can triple incident response volume and reduce time to response significantly.

> # Given the widening cybersecurity skills gap, the rising cost of a data breach and the blinding speed at which alerts pile up in SIEM logs, security leaders must empower their analysts

"While data breach costs have been rising steadily, we see positive signs of cost savings through the use of newer technologies as well as proper planning for incident response, which can significantly reduce these costs," said Dr. Larry Ponemon.

Automation reduces the average cost of a data breach by USD 1.55 million. To build a cyber resilient enterprise, security leaders need intelligent solutions for orchestration, automation, machine learning and artificial intelligence (AI).

■ What Are the Attributes of

Intelligent Incident Response?
Enterprises can save an average of USD 1 million by containing a data breach in under 30 days, according to the Ponemon study. However, the average time to containment is 69 days. Security leaders should consider the risks of failing to adopt solutions to for intelligent and proactive response, including costlier data breaches caused by reactive response and longer containment times.

The SOC is facing a higher volume of more sophisticated threats, and there is a massive shortage of cybersecurity talent to boot. The right approach to intelligent response, therefore, encompasses solutions for the following:

1. Orchestration and automation — An integrated, streamlined ecosystem can enable organizations to create dynamic incident response (IR) plans and automate remediation.

2. Human and artificial intelligence — Operationalize human intelligence, leverage advanced threat intelligence and collaborate with experts.

3. Case management — Establish systems for continual IR plan improvement while developing a clear understanding of internal workloads and skills.

Let's take a closer look at how intelligence incident response orchestration works in practice and how it can help security leaders free up their overworked analysts for more pressing tasks.

■ 3 Use Cases for Intelligent Incident Response Orchestration
A comprehensive ecosystem of security solutions can enable the enterprise to prepare for sophisticated cyberthreats, respond proactively to risks and apply lessons learned to create future safeguards. Intelligent orchestration creates efficiency and accuracy before an attack, during an incident and after remediation.

1. Before an Attack: Half of

respondents to a recent survey believe it's somewhat or highly likely that their organization will have to respond to a major incident in the next year, while 9% have "no doubt." The right time to address SOC challenges, such as the increased volume of highly targeted threats and too many single-purpose solutions, is before an attack occurs.

The first step to build a cyber resilient enterprise involves adopting an advanced incident response platform to create automated, intelligent workflows that encompass people, processes and technology. This solution can be enhanced with a security information and event management (SIEM) solution to deliver comprehensive incident analytics and visibility into emerging threats.

Enlisting security operations consultants can help organizations supplement their internal talent. Collaborating with external IR experts, meanwhile, can help companies implement effective training and strategic preparation.

2. During an Attack: Minutes count when the enterprise is facing a sophisticated, targeted threat. The incident response platform (IRP) can act as a centralized solution for comprehensive response remediation. When coupled with cognitive intelligence, organizations can rapidly investigate threats without overwhelming their SOC staff.

When a critical incident is detected, the SOC can call in on-demand IR experts for assistance managing and remediating the incident. The IRP generates a response playbook, which updates dynamically as threat intelligence solutions provide analysis of the incident and endpoint analytics solutions deliver details of on-site infection and automated reporting to the legal team.

Using solutions for threat intelligence, forensics and other solutions, IR analysts can research the tactics used by attackers to pinpoint the source of the incident. By following instructions from the playbook, SOC analysts can coordinate with IT on remediation actions, such as global password resets and segregation of privileged accounts.

3. After an Attack: There are few genuinely random cybersecurity attacks. In the last 18 months, 56% of organizations that fell victim to a significant attack were targeted again in the same period.

When an attack is fully remediated, security analysts can prepare efficient reporting on the incident using data from security intelligence solutions, forensic investigation tools and insights from the response researchers. This research can be presented directly to the executive leadership team to communicate the status of the incident, actions taken and lessons learned.

By collaborating with third-party response experts and security service consultants, the SOC team can work to refine formal incident response policies and enhance security controls. As SOC operations resume, analysts can improve readiness with a customized response drill training.

■ Why Incident Response Orchestration Matters

By protecting the enterprise with solutions to automate and orchestrate incident response, security leaders can introduce the benefit of cyber resiliency to the organization. According to Forrester, "Technology products that provide automated, coordinated, and policy-based action of security processes across multiple technologies, [make] security operations faster, less error-prone, and more efficient." Adding the right solutions for orchestration, cognitive intelligence, and case management can ease the burden on the SOC while reducing cybersecurity risks■

The author is Content Marketing Manager at IBM Resilient

Can The CIO Become The CEO Or COO?

Some of them have. Already.

Can the CIO become CEO or COO? This question has been asked rhetorically many times to make a point that CIOs are now taking business decisions and are thinking like business managers, making them 'potential' COOs/CEOs like any other business manager.

The fact that many of them have taken other functional roles have only fueled the discussion. Some of the top CIOs who also handle other functions in their respective companies include Rajesh Uppal, erstwhile CIO of Maruti, who is now Executive Director (HR & IT) at his company; Vijay Sethi, CIO, Head HR and Head CSR at Hero Motocorp; Manish Choksi, who headed IT and Corporate strategy at Asian Paints. These are just examples from largest corporations. There are more in the list.

There are, of course, CIOs and CISOs, in IT/telecom companies who have been given additional/new charge of business lines. It is fairly common in IT services industry.

However, there are only a few CIOs who have become full-fledged COOs and CIOs ■

Before him, some four years back, **Rajesh Munjal** took over as the COO of Carzonrent that operates the Easycabs taxi services. He was the CIO of the company before taking up the role of director, business operations and finally becoming the COO.

The most high-profile CIO-turned-CEO case is that of **Ashish Chauhan**, the current CEO of Bombay Stock Exchange (BSE). He was formerly the CIO of Reliance Industries and Reliance Infocom. He also headed Mumbai Indians IPL team as CEO for some time.

Mridul Sharma, who has just taken over as the COO of Kirloskar Capital was EVP & Head of Technology before taking over the COO role. He has served in technology roles in Barclays Bank and Tata AIG General Insurance.

Another radio taxi operator, Meru Cabs, also has an erstwhile CIO at the helm, this time as CEO. **Nilesh Sangoi**, who is the CEO of Meru Cabs, headed technology for the company earlier.

India Among Top Nations Leading GDPR Readiness: Study

India stood sixth globally with 65% of Indian organizations showing higher preparedness towards meeting most or all of the GDPR requirements

ndia finds its place amongst the leading nations globally in their preparedness towards the General Data Protection Regulation (GDPR), according to Cisco's *2019 Data Privacy Benchmark Study*.

According to the study, organizations worldwide that invested in maturing their data privacy practices are now realizing tangible business benefits from these investments. The study

Source: Cisco 2019 Data Privacy Benchmark Study
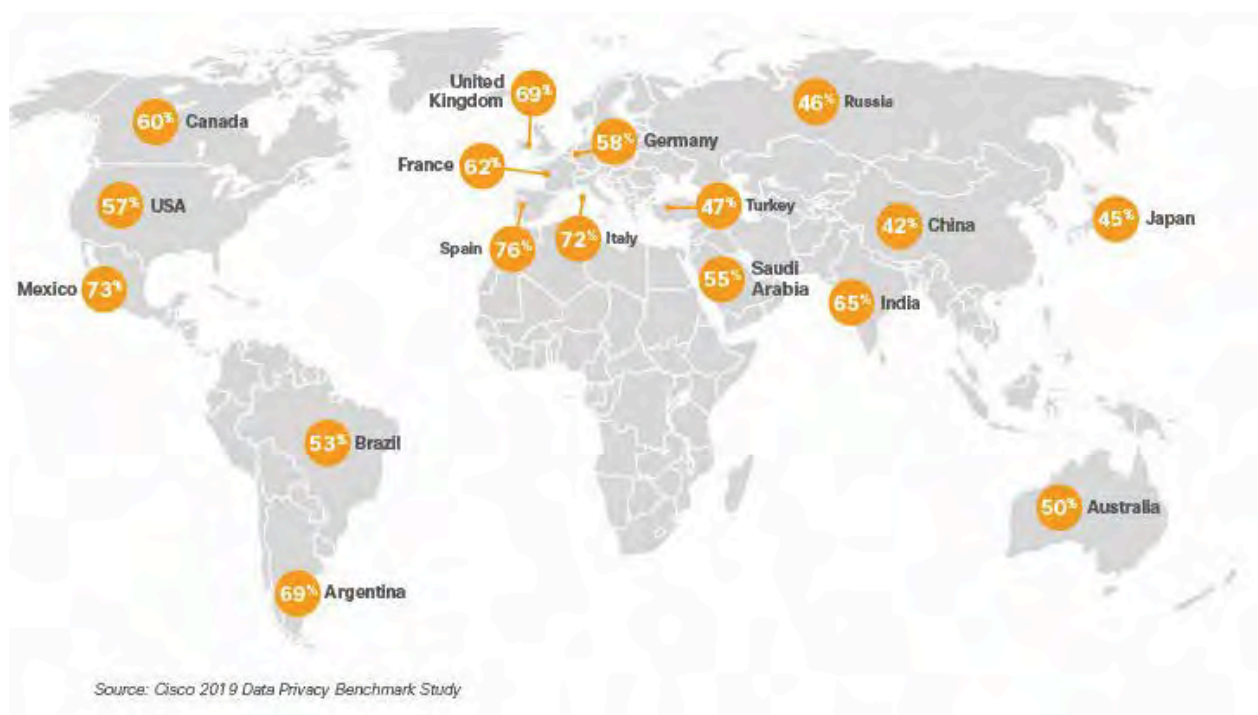
validates the link between good privacy practice and business benefits as respondents report shorter sales delays as well as fewer and less costly data breaches.

The European Union's General Data Protection Regulation, which focused on increasing protection for EU residents' privacy and personal data, became enforceable in May 2018. Organizations worldwide have been working steadily towards getting ready for GDPR. Within Cisco's *2019 Data Privacy Benchmark Study*, 59% of organizations reported meeting all or most requirements, 29% expect to do so within a year, and 9% will take more than a year. (See Figure 1) Interestingly, India stood sixth globally with 65% of Indian organizations showing higher preparedness towards meeting most or all of the GDPR requirements.

"This past year, privacy and data protection importance increased dramatically. Data is the new currency, and as the market shifts, we see organizations realizing real business benefits from their investments in

protecting their data," said Michelle Dennedy, Chief Privacy Officer, Cisco.

Customers are increasingly concerned that the products and services they deploy provide appropriate privacy protections. Those organizations that invested in data privacy to meet GDPR experienced shorter delays due to privacy concerns in selling to existing customers: 3.4 weeks vs. 5.4 weeks for the least GDPR ready organizations. Overall the average sales delay was 3.9 weeks in selling to customers, down from 7.8 weeks reported a year ago.

Vishak Raman, Director, Security, Cisco said, "India has greatly improved upon its GDPR readiness with its fast evolving data privacy ecosystem, which is primarily because of a collaborative approach by the government and private organizations. However, there remains a huge scope for Indian organizations to increase their investments in people, and technology controls to meet customer privacy requirements faster."

GDPR-ready organizations cited

Those organizations that invested in data privacy to meet GDPR experienced shorter delays in selling to existing customers: 3.4 weeks vs. 5.4 weeks for the least GDPR ready organizations

a lower incidence of data breaches, fewer records impacted in security incidents, and shorter system downtimes. They also were much less likely to have a significant financial loss from a data breach. Beyond this, 75% of respondents cited that they are realizing multiple broader benefits from their privacy investments, which

Figure 1: **GDPR Readiness**

% of respondents, N = 3206

■ Currently meeting most/all of of the GDPR requirements

■ Not yet meeting most/all GDPR requirements, and it will take more than a year

■ Not yet meeting most/all GDPR requirements, but we expect to within a year

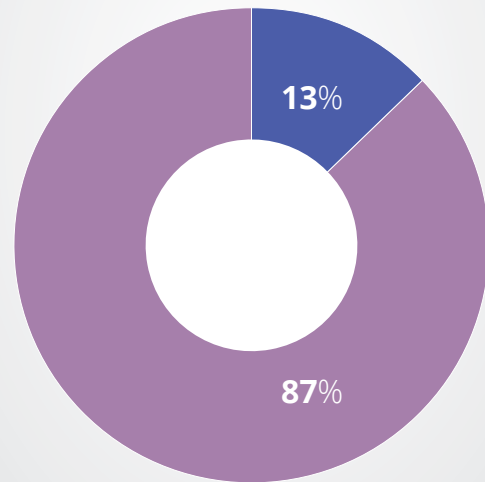■ Not applicable-GDPR doesn't really apply to us
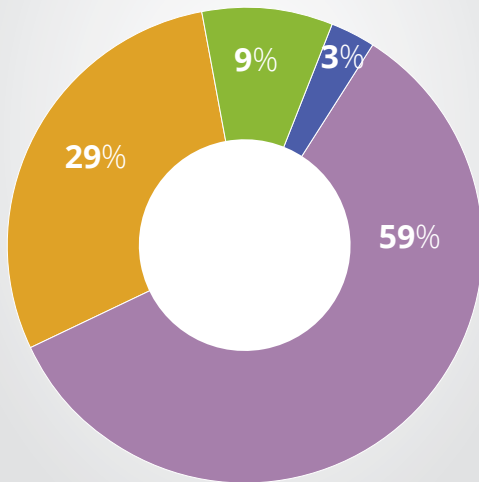
Source: Cisco 2019 Data Privacy Benchmark Study, n=3206

Figure 2: **Respondents Experiencing Delays in their Sales Cycles due to Customers'**

% of respondents, N = 2064

■ Yes ■ No

Source: Cisco 2019 Data Privacy Benchmark Study

include greater agility and innovation resulting from having appropriate data controls, gaining competitive advantage, and improved operational efficiency from having data organized and catalogued.

More than 3,200 global security and privacy professionals in 18 countries across major industries responded to the Cisco survey about their organizations' privacy practices. Key findings include:

■ 87% of companies are experiencing delays in their sales cycle due to customers' or prospects' privacy concerns, up from 66% last year. This is likely due to the increased privacy awareness brought on by GDPR and the frequent data breaches in the news. (See Figure 2)

■ Sales delays by country varied from 2.2 to 5.5 weeks, with Italy, Turkey and Russia at the lower end of the range, and Spain, Brazil and Canada at the higher end. Longer

87% of companies are experiencing delays in their sales cycle due to customers' or prospects' privacy concerns, up from 66% last year. This is likely due to the increased privacy awareness brought on by GDPR

sales delays can be attributed to areas where privacy requirements are high or in transition. Delayed sales can

cause revenue shortfalls related to compensation, funding, and investor relations. Delayed sales also can become lost sales if a potential customer buys from a competitor or decides not to buy at all.

■ Top reasons cited for sales delays included investigating customer requests for privacy needs, translating privacy information into customer languages, educating customers about an organization's privacy practices, or redesigning products to meet customer privacy needs.

■ By country, GDPR-readiness varied from 42% to 76%. Spain, Italy, UK and France were at the top of the range, while China, Japan and Australia were on the lower end. (See Figure 3)

■ Only 37% of GDPR-ready companies experienced a data breach costing more than USD 500,000, compared with 64% of the least GDPR-ready companies■

Cryptominers Led Cyberattacks In 2018

This is followed by mobile malware, botnet malware, banking malware and ransomware

37% organizations have been affected by cryptominers globally, followed by mobile malware (33%), botnet malware (18%), banking malware (13%) and ransomware (4%), according to Checkpoint's *Cyber Attack Trends Analysis Security Report 2019*.
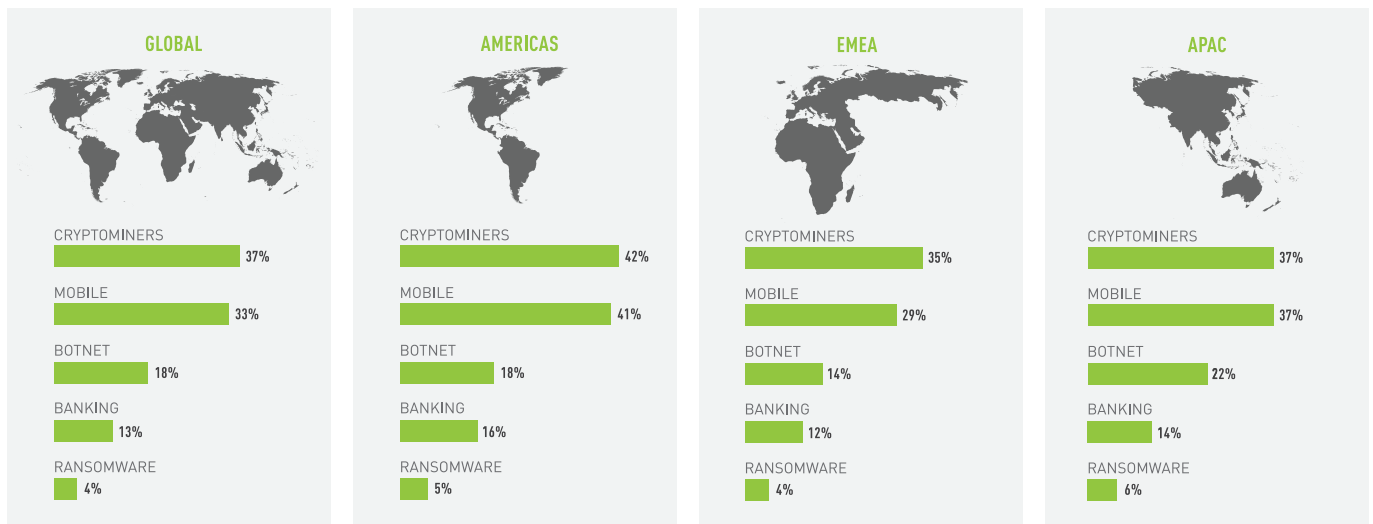
The report indicates although there is rise in cryptomining attacks, there is a sharp decline in the ransomware attacks. (See Figure 1)

Checkpoint outlines key cyber threats which affected organizations globally in 2018:

Crytominers dominated in 2018

Cryptomining attacks soared in 2018, affecting over 40% of organizations worldwide at its peak, compared to 20.5% at the end of 2017, and dominated the top cyberattacks and malware families. In January 2018, total cryptocurrency values dropped rapidly, shrinking by about 86% from their peak. Despite this, cryptominers detached themselves from cryptocurrencies' market cap and kept their place as the most prominent malware infection used by threat actors in 2018.

Figure 1: **Top cyber attack categories globally and by region**

	GLOBAL	AMERICAS	EMEA	APAC
CRYPTOMINERS	37%	42%	35%	37%
MOBILE	33%	41%	29%	37%
BOTNET	18%	18%	14%	22%
BANKING	13%	16%	12%	14%
RANSOMWARE	4%	5%	4%	6%

Source: Checkpoint's Cyber Attack Trends Analysis Security Report 2019

Mobiles, a moving target

33% of organizations worldwide were hit by mobile malware, with the leading three malware types targeting the Android OS. 2018 saw several cases where mobile malware was pre-installed on devices, and apps available from app stores that were actually malware in disguise. Hiddad, an ad-distributing malware for Android that can bypass the Google Play Protect verification system, is back in the top ranks as the top mobile malware globally, as well as in the APAC and EMEA. Guerilla is a new mobile malware family embedded in multiple legitimate apps and can download additional malicious payloads to generate fraudulent ad revenue.

Multi-purpose botnets

Bots were the third most common malware type, with 18% of organizations hit by bots which are used to launch DDoS attacks and spread other malware. Bot infections were instrumental in nearly half (49%) of organizations experiencing a DDoS attack in 2018. The notorious Necurs, which first emerged in 2012, is at the head of the top global, Americas and EMEA ranks, and is one of the most prevalent botnets of 2018. This year, the giant spam botnet adopted new techniques to avoid detection, targeted banks, was behind a variety of email scams, and pushed various payloads including cryptominers, ransomware, banking Trojans, and RATs. Dorkbot is another prominent botnet which dominated the charts. It reached the top of APAC ranks, and also ranked second in the EMEA and globally.

Banks still not spared

13% organizations have been affected by banking malware in 2018. Ramnit is the most prominent banking Trojan of the past year. It first appeared in 2010 and has remained active ever since. Ramnit's popularity is in line with the exposure by Check Point researchers of a massive new 'Black' campaign based on the banker. The campaign turned the victim machines into malicious proxy servers and resulted in over 100,000 infections. Shortly after the 'Black' campaign was shut down, a new Ramnit campaign emerged, distributing the AZORult info-stealer and downloader, via the RIG and Grand-Soft Exploit Kits. Trickbot is another dominant banking Trojan widely observed in 2018 that reached the top of the global, Americas and EMEA rankings.

Ransomware in decline

2018 saw ransomware usage fall sharply, impacting just 4% of organizations globally. This is down from 30% in 2017. This shift may be the result of the move to cryptomining as a more efficient and profitable alternative. It can also be related to the adoption of the 'boutique' ransomware attacks that only target specific organizations instead of wide global campaigns. "From the meteoric rise in cryptomining to massive data breaches and DDoS attacks, there was no shortage of cyber-disruption caused to global organizations over the past year. Threat actors have a wide range of options available to target and extract revenues from organizations in any sector, and the first instalment of the 2019 Security Report highlights the increasingly stealthy approaches they are currently using," says Peter Alexander, Chief Marketing Officer of Check Point Software Technologies■

Cyberattacks Rise In 2018: Study

A Skybox Security study reveals a 12% increase in Common Vulnerabilities and Exposures (CVEs) in 2018 as compared to 2017

There is significant rise in the volume of new vulnerabilities in 2018, according to Skybox Security's Vulnerability and Threat Trends Report. The National Vulnerability Database (NVD) assigned 16,412 new Common Vulnerabilities and Exposures (CVEs), a 12% increase over the previous year. That may seem like a small climb, but the 2017 figure was already an all-time high, and Skybox Director of Threat Intelligence Marina Kidron believes these record-breaking figures are the new normal.

"It would come as no surprise if 2019 breaks the CVE record again," said Kidron. "While more resources in vulnerability research is what's driving these high numbers, that's cold comfort to CISOs trying to keep their organization safe. The challenge of answering, 'What do I fix today?' is only getting harder—unless you have the right information to contextualize this mountain of data. That's what drives the work we're doing and why we publish the report."

Ron Davidson, Skybox CTO and Vice President of R&D, echoed a similar sentiment: "If you're hanging your vulnerability management strategy on fixing CVSS critical- or high-severity vulnerabilities, 2018 added about 9,000 vulnerabilities to that list; it's simply no longer practical to 'focus' attention on this large group. Exploitability — what's being used in the wild, what sample code is available — is a more important indicator of what should get attention first. It's something many vulnerability management programs lack, so their resources are going in the wrong place and they're not moving the needle on risk."

Other findings of the report include risks to the growing attack surface, including operational technology (OT) networks. Attacks on OT continue to climb with a 10% increase between 2017 and 2018. While these attacks range in motive and impact, the WannaCry outbreak in Taiwan Semiconductor Manufacturing Company was a prime example of how a cybercriminal tool like ransomware, nation-state threats and internal exposure can create the perfect storm to wreak havoc on a network, as well as a company's bottom line.

The report also warns of a false sense of security in cloud networks. While the security of clouds is relatively strong, misconfiguration issues within them can still abound and security issues can arise within the applications used to manage such networks.

A number of examples can be given of attacks on cloud networks, but a notable one from 2018 targeted Tesla's Amazon Web Services network. While attackers could have accessed a variety of information, they instead used the opportunity to launch a malicious cryptominer, pointing to a larger trend in the threat landscape of stealing computational power rather than data. In 2017, ransomware reigned supreme accounting for 28% of malware attacks, while cryptominers only made up 9%. Those figures essentially flipped in 2018, with ransomware dropping to 13% of malware attacks and cryptominers soaring to 27%.

"While cryptomining may seem like a relatively innocuous, low-priority threat, it's important to remember that these attacks slow down system processes and may overwhelm system capacity," said Skybox Senior Security Analyst Sivan Nir."■

Key Cybersecurity Threats

That Will Impact APAC Organizations In 2019

One of the threats will be a surge in the number of vulnerabilities in AI and chatbots

2018 has been another transformative time for security teams in APAC regions. The imposition of new regulations like Australia's Notifiable Data Breaches scheme and the Indian government's push to be GDPR compliant due to recent global breaches, have been influential on cybersecurity investment and strategy. Along with a rise in the number of incidents of data theft and cyberattacks in India and a workforce bogged down compliance management, 2018 has been another challenging year for cybersecurity and business leaders. But does 2019 face the same fate? Skybox Security outlines predictions for the year ahead:

■ **Crypto-jacking keeps going:** 2018 saw unauthorized cryptomining replace ransomware as the most popular malware, and this will not abate. Monero has been identified as the cryptocurrency which is most associated with this activity. This type of malware can often go around undetected, and it's a good way for hackers to stay active for the maximum amount of time and make quick money. Why would they turn to an alternative?

■ **Mobile vulnerabilities keep rising:** A continuing trend which emerged at the end of 2017 is the exponentially growing number of mobile vulnerabilities. This is only going to continue as mobile further blurs the line between personal and business device. Furthermore, third-party applications used on smart phones are a good way for malware to enter an organization, as well as open applications, particularly Android.

■ **Cloud misconfigurations cause chaos:** As more and more companies migrate to the cloud, the biggest risk will be seen in the misconfiguration of the cloud environment, showing that humans continue to be one of the weakest links in security. In addition, the incorporation of third-party software in the cloud means organizations won't have full control over their attack surface. Cloud technology is still relatively new, with no set best practices, so it's not as clear to IT people how to secure a cloud environment as opposed to on-prem networks. Next year, hackers will take more advantage of these weaknesses.

■ **Ransomware won't fade away:** 2017 will always be remembered as the 'year of ransomware'. While cryptomining is overshadowing ransomware, it's important that CISOs don't let their guard drop on this older threat. Although illicit cryptomining is easier to undertake, ransomware has the potential to reap bigger immediate awards when precisely targeted at an organization that cannot afford to kiss their encrypted files goodbye. So, ransomware will continue to wreak havoc, using a variety of new techniques to enter the network.

■ **AI arms race:** AI will be increasingly used to identify and protect against attacks, but 2019 will see a surge in the number of vulnerabilities in AI and chatbots as threat actors realize the value in this activity. Hackers will begin to use AI to make more efficient and persistent malware attacks. At some level this may even culminate in an AI cyber-arms race. There will be more investment being ploughed into cyber-AI on both sides of the battlefield■

Cloud Infrastructure Services Spending Rises In Q4, 2018; Amazon Still On Top: Study

A Synergy Research Group (SRG) study reveals a jump of 45% from the fourth quarter of 2017, giving a full-year growth rate of 48% in 2018

The Q4 spend on cloud infrastructure services jumped 45% from the fourth quarter of 2017, giving a full-year growth rate of 48% in 2018, according to Synergy Research Group (SRG). Notably the growth rates seen throughout 2018 were higher than those achieved in 2017. Amazon, the clear market leader, nudged its market share upwards and remains equivalent in size to its next four competitors combined. Meanwhile revenue growth at Microsoft, Google and Alibaba again far surpassed overall market growth rate, so all three gained substantial market share, with Microsoft in particular jumping ahead. The market share gains of these four were primarily at the expense of small-to-medium sized cloud operators, who collectively have lost five percentage points of market share over the last four quarters. Many of those smaller players are still growing revenues but find themselves unable to keep pace with the market leaders. Among the leaders, IBM's prime focus is a little different from the others as it remains the strong leader in the hosted private cloud services segment of the market.

With most of the major cloud providers having now released their earnings data for Q4, Synergy estimates that quarterly cloud infrastructure service revenues (including IaaS, PaaS and hosted private cloud services) were approaching USD 20 billion, giving a full-year total of almost USD 70 billion. Public IaaS and PaaS services account for the bulk of the market and those grew by 49% in Q4. In public cloud the dominance of the top five providers is even more pronounced, as they control over three quarters of the market. Geographically, the cloud market continues to grow strongly in all regions of the world.

"Q4 tops off a banner year for the cloud market with the annual growth rate actually nudging up from the previous year, which is an unusual phenomenon for a high-growth market of this scale," said John Dinsdale, a Chief Analyst at Synergy Research Group. "The rate at which the market leaders continue to expand is really rather impressive. In aggregate the top five drove up their revenues in these segments by 60% in 2018, which has caused us to review and increase our five-year forecast for the market. Inevitably there will be a few road bumps along the way but these will be minor relative to the factors that continue to drive the market."▪

Cloud Infrastructure Services - Market Share
(IaaS, PaaS, Hosted Private Cloud)

Source: Synergy Research Group

Worldwide Market Share

Legend: Q4 2018, Q4 2017
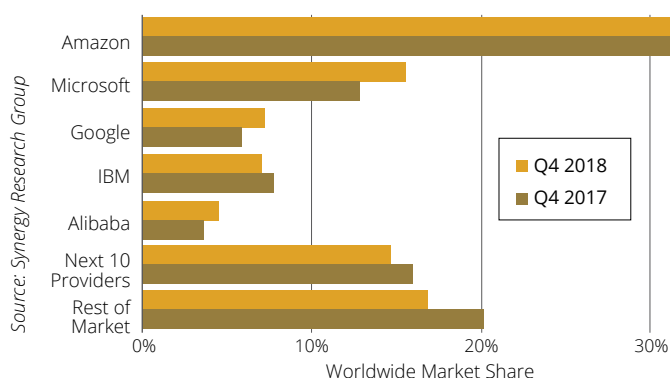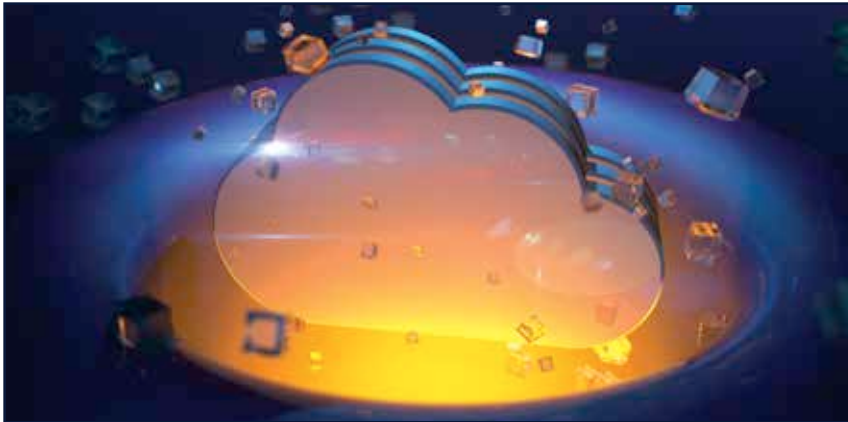
Total Collaboration Market To Rise In 2019; Cisco Still On Top: Study

A Synergy Research Group (SRG) study shows the growth to be 9% and reach over USD 45 billion, driven by a group of high-growth hosted & cloud collaboration market segments

The total collaboration market will grow by 9% in 2019 to reach over USD 45 billion, driven by a group of high-growth hosted & cloud collaboration market segments, according to a Synergy Research Group study. TeamWork Apps will be the highest growth market, up by almost 60% in 2019, while CPaaS and VaaS will each grow by around 30%, with UCaaS and CCaaS being the next highest growth markets. In aggregate, total hosted & cloud collaboration markets will grow by 19% in 2019 while revenue from on-premise products will decline by 3%. Quarterly vendor revenues from collaboration are now running at an all-time high and are projected to continue growing steadily over the next five years. Cisco maintained its lead in the total collaboration market and in

the last quarter it pulled further ahead of second-ranked Microsoft. Beyond these leaders, the vendors who are growing the most rapidly include Slack,

twilio, BroadCloud (Cisco), Zoom, Fuze, Dropbox, RingCentral and LogMeIn (Jive) – companies that are leading the charge in the high-growth segments. The growth of Slack is particularly noteworthy as it has more than doubled in size year over year.

Total worldwide Q3 revenues from collaboration – which include a range of both on-premise products and hosted/cloud communications and applications – were just shy of USD 11 billion and Q4 revenues will be substantially higher. Revenues from hosted/cloud solutions now account for 64% of the total and on-premise products 36%, a marked change from twelve quarters ago when the market was split evenly between the two. North America continues to account for just over half of the total market and the EMEA region just under a third.

"Collaboration continues to be a somewhat fragmented market with many disruptive and high-growth companies targeting specific technology areas," said Jeremy Duke, Synergy Research Group's founder and Chief Analyst. "That being said, the overall trend is quite clear in that traditional on-premise sales are shrinking and being replaced by cloud-based communication services. There is now wide adoption of these new emerging cloud services and our forecasts show that they will continue to grow strongly over the next five years."■

UC Collabration Market Growth
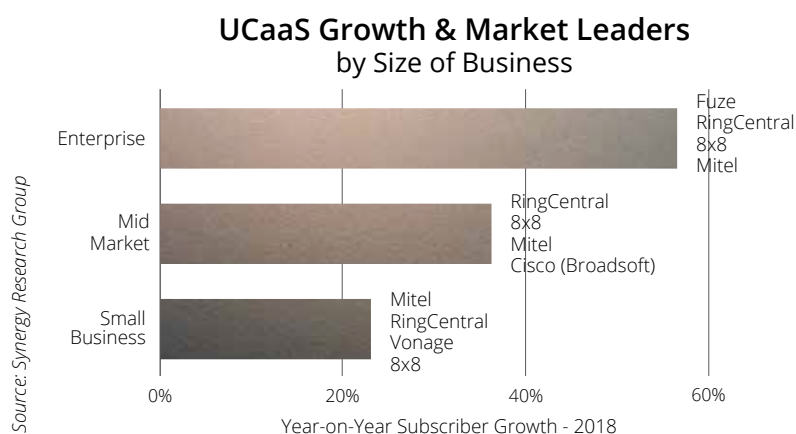

Source: Synergy Research Group
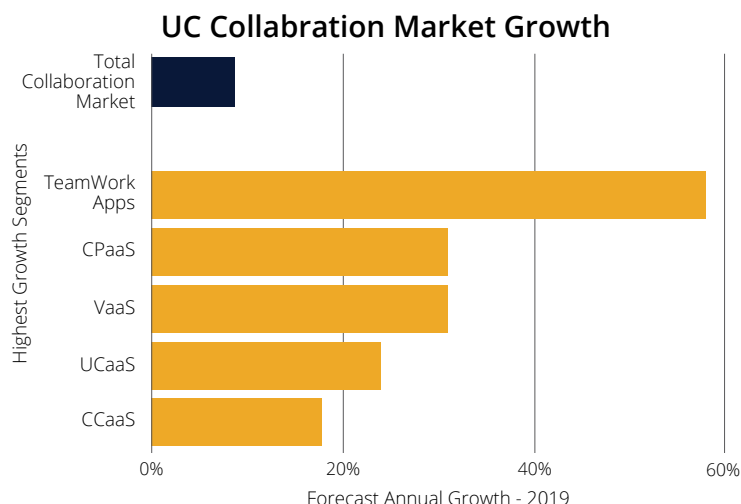
UCaaS To Grow Rapidly Over The Next Five Years: Study

A Synergy Research Group (SRG) study reveals UCaaS will grow by an average annual rate of 26% over the next five years, with growth being increasingly driven by enterprise customers

The installed base of UCaaS subscribers will grow by an average annual rate of 26% over the next five years, with growth being increasingly driven by enterprise customers, according to Synergy Research Group (SRG). Small and mid-sized businesses still account for almost 90% of all UCaaS subscribers, but the enterprise segment is growing far more rapidly. In 2018 the number of enterprise UCaaS subscribers grew by 57% while the mid-market and small business segments grew by 36% and 23% respectively. In terms of UCaaS service providers, each segment had a different market share leader, with Fuze leading in enterprise, RingCentral in mid-market and Mitel in small business. Other notable UCaaS providers include Cisco (Broadsoft), 8x8, Vonage, LogMeIn and Broadview.

Total UCaaS subscriber numbers are now well over the eight million mark and have doubled since late 2015, with the market split between retail and

UCaaS Growth & Market Leaders
by Size of Business

Source: Synergy Research Group

Enterprise — Fuze / RingCentral / 8x8 / Mitel

Mid Market — RingCentral / 8x8 / Mitel / Cisco (Broadsoft)

Small Business — Mitel / RingCentral / Vonage / 8x8

Year-on-Year Subscriber Growth - 2018

wholesale business models. On the larger retail side RingCentral and 8x8 are the leading providers and in the wholesale Mitel and Cisco/Broadsoft lead. The worldwide market continues to be dominated by the US, with market development still being in the early days in most other countries.

"UCaaS took off in the small and mid-market segments first. We are now seeing UCaaS growth rates in small businesses start to tail off a little, while

growth in the mid-market remains strong. But it is in the nascent enterprise segment where UCaaS growth is really booming," said Jeremy Duke, Synergy Research Group's founder and Chief Analyst. "UCaaS penetration of the PBX installed base has barely passed the 10% mark so we project continued strong growth throughout the forecast period. UCaaS growth will be particularly strong in the enterprise market and also in countries beyond the US."■

Gartner Debunks Five Artificial Intelligence Misconceptions

IT and business leaders developing AI projects must separate reality from myths to devise their future strategies

T and business leaders are often confused about what artificial intelligence (AI) can do for their organizations and are challenged by several AI misconceptions. According to Gartner, IT and business leaders developing AI projects must separate reality from myths to devise their future strategies.

"With AI technology making its way into the organization, it is crucial that business and IT leaders fully understand how AI can create value for their business and where its limitations lie," said Alexander Linden, research vice president at Gartner. "AI

technologies can only deliver value if they are part of the organization's strategy and used in the right way."

Gartner has identified five common myths and misconceptions about AI:

Myth No.1: AI Works in the Same Way the Human Brain Does

AI is a computer engineering discipline. In its current state, it consists of software tools aimed at solving problems. While some forms of AI might give the impression of being clever, it would be unrealistic to think that current AI is similar or equivalent to human intelligence.

"Some forms of machine learning (ML) – a category of AI - may have been inspired by the human brain, but they are not equivalent," Linden said. "Image recognition technology, for example, is more accurate than most humans, but is of no use when it comes to solving a math problem. The rule with AI today is that it solves one task exceedingly well, but if the conditions of the task change only a bit, it fails."

Myth No. 2: Intelligent Machines Learn on Their Own

Human intervention is required to develop an AI-based machine or system. The involvement may come from experienced human data scientists who are executing tasks such as framing the problem, preparing the data, determining appropriate datasets, removing potential bias in the training data (see myth No. 3) and – most importantly- continually updating the software to enable the integration of new knowledge and data into the next learning cycle.

Myth No. 3: AI Can Be Free of Bias

Every AI technology is based on data, rules and other kinds of input from human experts. Similar to humans, AI is also intrinsically biased in one way or the other. "Today, there is no way to completely banish bias,

however, we have to try to reduce it to a minimum," Linden said. "In addition to technological solutions, such as diverse datasets, it is also crucial to ensure diversity in the teams working with the AI, and have team members review each other's work. This simple process can significantly reduce selection and confirmation bias."

Myth No. 4: AI Will Only Replace Repetitive Jobs That Don't Require Advanced Degrees

AI enables businesses to make more accurate decisions via predictions, classifications and clustering. These abilities have allowed AI-based solutions to replace mundane tasks, but also augment remaining complex tasks.

An example is the use of imaging AI in healthcare. A chest X-ray application based on AI can detect diseases faster than radiologists. In the financial and insurance industry, robo advisors are being used for wealth management or fraud detection. Those capabilities don't eliminate human involvement

in those tasks but will rather have humans deal with unusual cases. With the advancement of AI in the workplace, business and IT leaders should adjust job profiles and capacity planning as well as offer retraining options for existing staff.

Myth No. 5: Not Every Business Needs an AI Strategy

Every organization should consider the potential impact of AI on its strategy and investigate how this technology can be applied to the organization's business problems. In many ways, avoiding AI exploitation is the same as giving up the next phase of automation, which ultimately could place organizations at a competitive disadvantage.

"Even if the current strategy is 'no AI', this should be a conscious decision based on research and consideration. And – as every other strategy- it should be periodically revisited and changed according to the organization's needs. AI might be needed sooner than expected," Linden concluded.■

> "Today, there is no way to completely banish bias, however, we have to try to reduce it to a minimum... In addition to technological solutions, such as diverse datasets, it is also crucial to ensure diversity in the teams working with the AI..."

Majority Of Organizations To Adopt Mobile-Centric Biometric Authentication By 2022: Gartner

Lower costs and improved user experience/customer experience (UX/CX) are fuelling this increasing interest in biometric authentication

By 2022, 70% of organizations using biometric authentication for workforce access will implement it via smartphone apps, regardless of the endpoint device being used, according to Gartner. In 2018, this figure was fewer than 5%.

Lower costs and improved user experience/customer experience (UX/CX) are fuelling this increasing interest in biometric authentication.

"Security and risk management leaders responsible for identity and access management (IAM) and fraud prevention continue to seek approaches for identity corroboration that balance

trust and accountability against total cost of ownership and UX/CX," said Ant Allan, research vice president at Gartner. "Biometric authentication uses biological or behavioral traits unique to each person and offers better UX/CX and accountability than other common methods. Implementing this via smartphone apps provides more consistency in UX/CX and is technically simpler than supporting it directly on a variety of different endpoint devices."

Midsize and large organizations looking to implement biometric authentication via smartphone apps must be aware that biometric approaches that can be readily

supported on any smartphone are vulnerable to presentation attacks or "spoofing" using photos, videos, voice recordings, and so on. Therefore, presentation attack detection or "liveness testing" is essential.

SaaS-Delivered IAM Will Fulfill Most Needs

Gartner predicts that, by 2022, 40% of global midsize and larger organizations will use IAM capabilities delivered as software as a service (SaaS) to fulfill most of their needs — up from 5% in 2018.

SaaS-delivered IAM is often deployed to enhance access management software implementations. The ease of implementation and rapid time to value of SaaS-delivered IAM offerings have proved valuable to organizations that favor SaaS adoption and do not consider the operational management of IAM functionality core to their business.

"Based on our client interactions, most SaaS-delivered IAM purchases are for access management and lightweight identity governance and administration functionality, such as single sign-on. These offerings provide excellent connectivity and include solid access management and password management features," said Abhyuday Data, associate research principal analyst at Gartner. "B2B and B2C are the most established use cases with matured access management capabilities."

The steady movement of applications to cloud and mobile architectures is also influencing adoption. The combination of functional offerings that are configured, rather than customized, and modern application architectures is causing a substantial portion of the market to adopt SaaS-delivered IAM.

"Organizations looking to use SaaS-delivered IAM should first ensure they have established satisfactory and well-supported traditional IAM software stacks. They then need to consider SaaS-delivered IAM once functional needs are met and the organizational benefits are realized," concluded Data■

TO FOLLOW THE LATEST IN TECH,
FOLLOW US ON...

facebook.

digit.in/facebook

Majority Of Organizations Will Integrate AI To Aid Employees' Productivity By 2021: Gartner

This development will prompt 10% of organizations to add a digital harassment policy to workplace regulation

Artificial intelligence (AI) is increasingly making its way into the workplace, with virtual personal assistants (VPAs) and other forms of chatbots now augmenting human performance in many organizations. According to Gartner, by 2021, 70% of organizations will assist their employees' productivity by integrating AI in the workplace. This development will prompt 10% of organizations to add a digital harassment policy to workplace regulation.

"Digital workplace leaders will proactively implement AI-based technologies such as virtual assistants or other NLP-based conversational agents and robots to support and augment employees' tasks and productivity," said Helen Poitevin, senior research director at Gartner. "However, the AI agents must be properly monitored to prevent digital harassment and frustrating user experiences."

Past incidents have shown that poorly designed assistants cause frustration among employees, sometimes prompting bad behavior and abusive language toward the VPA. "This can create a toxic work environment, as the bad habits will eventually leak into interactions with co-workers," said Poitevin.

Recent experiments have also shown that people's abusive behavior toward AI technologies can translate into how they treat the humans around them. Organizations should consider this when establishing VPAs in the workplace and train the assistants to respond appropriately to aggressive language.

Poitevin added: "They should also clearly state that AI-enabled conversational agents should be treated with respect, and give them a personality to fuel likability and respect. Finally, digital workplace leaders should allow employees to report observed cases of policy violation."

Back-Office Bank Employees Will Rely on AI for Non-routine Work

According to Gartner, by 2020, 20% of operational bank staff engaged in back-office activities will rely on AI to do non-routine work.

"Non-routine tasks in the back offices of financial institutions are things like financial contract review or deal origination," said Moutusi Sau, senior research director at Gartner. "While those tasks are complex and require manual intervention by human staff, AI technology can assist and augment the work of the staff by reducing errors and providing recommendation on the next best step."

AI and automation have been applied to routine work that has been successful across banks and their value chain. "In some cases, we witnessed layoffs to reduce unneeded head count, and understandably back-office staff are worried their jobs will be replaced by machines," said Sau.

However, AI has a bigger value-add than pure automation, which is augmentation. "The outlook for AI in banking is in favor of proactively controlling AI tools as helpers, and those can be used for reviewing documents or interpreting commercial-loan agreements. Digital workplace leaders and CIOs should also reassure workers that IT and business leaders will 'deploy AI for good'," concluded Sau■

CFO INDIA

NETWORK

Intelligence . Leadership . Transformation

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

Double Scoop

Two times the revelation

MY FAVORITE SPORT

Cricket

A TECH SHOW I ATTENDED RECENTLY

NASSCOM DSCI

A MOVIE I WOULD LOVE TO WATCH REPEATEDLY

3 Idiots

MY FAVORITE CUISINE

Indian

Sandip Sannyasi
Senior Manager - IT
Dell Technologies

MY FAVORITE TECH BOOK

Steve Jobs: The Man Who Thought Different: A Biography

MY PEER IN THE IT COMMUNITY

Ashish B Adhvaryu
Director - CSFC Delivery, HCL

MY FAVORITE DRESS

Blazer

MY FAVORITE AUTHOR

Ravi Subramanium

A TECH TOOL WHICH I FREQUENTLY USE

Microsoft PowerPoint

MY FAVORITE SINGER

Kishore Kumar

A TECH IDOL WHOM I WOULD LOVE TO MEET

Bill Gates

CFO
INDIA

N E T W O R K
Intelligence . Leadership . Transformation

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