SILLY POINT
Spotlight: Spatial Computing Pg 18

5G
5G: A catalyst for enterprise transformation Pg 34

Volume 11
Issue 09
Nov-Dec 2022
₹150

CIO&LEADER

TRACK TECHNOLOGY•BUILD BUSINESS•SHAPE SELF

Cybersecurity in 2023:

What's keeping tech honchos up at night?

The top cybersecurity challenges are driven by the organization's ever-growing hybrid workforce culture and digital footprint.
pg. 10

A 9.9 Group Publication

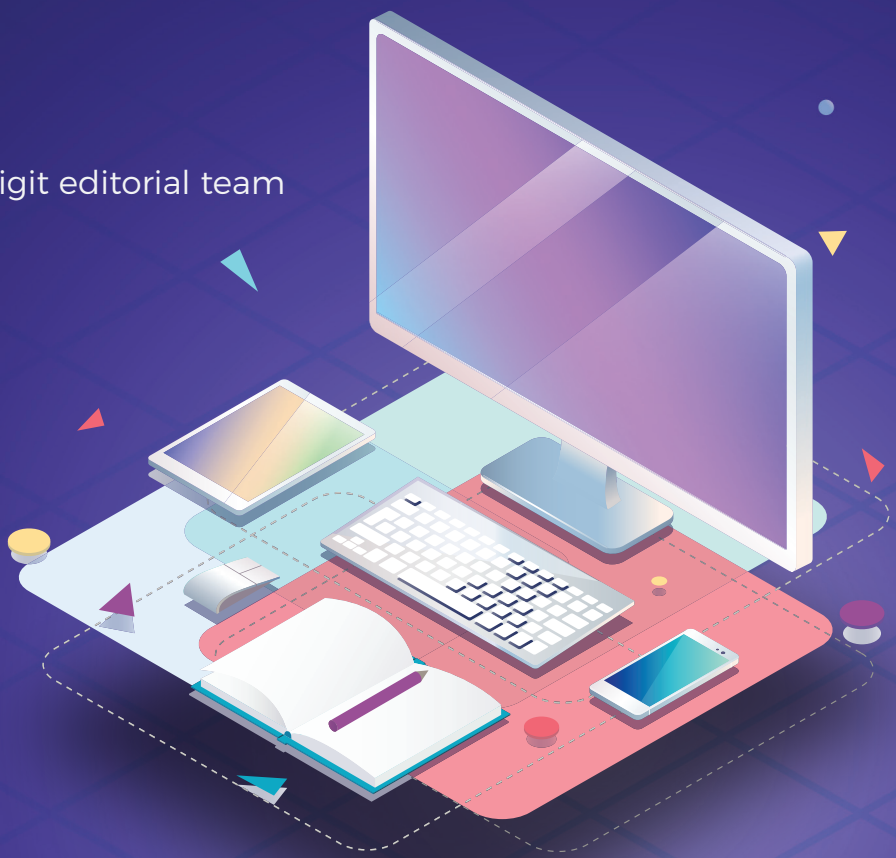
LAUNCHING

digit SQUAD

Here is your chance to become a Digit certified tech influencer

Benefits of Digit Squad Member

- Launch your own tech channel on Digit.in
- Become a Digit Certified tech influencer
- Engage with digit editorial team
- Make money



Apply now by scanning the QR code

www.digit.in/digit-squad/apply.html

EDITORIAL

Shyamanuja Das
shyamanuja.das@9dot9.in

The 2023 Priorities

ChatGPT of OpenAI is the flavour of the season. Like everybody else, who has some interest in artificial intelligence and machine learning, I also tried to test the chatbot for fun. .

No mark for guessing what I asked - what are the priorities for Indian CIOs in 2023?

While admitting that it is difficult to predict with certainty, what the priorities for Indian CEOs will be in 2023, ChatGPT, however, threw four priorities, what it called, 'potential areas of focus' for Indian CEOs in 2023'. On top of the list, of course, was digital transformation. On number two position was cyber security.

"As more organizations in India adopt digital technologies, CIOs may need to prioritise cyber security to protect sensitive data and prevent cyberattacks. This could involve implementing strong security protocols and monitoring systems to detect and respond to potential threats.'

It is a direct quote from ChatGPT's answer. Based on training data, it may or may not be an accurate forecast. But it is a good indicator of what most people think, say and write.

"Cyber security is increasingly resembling a competitive strategy game, with the stakes rising as the bar is raised."

When I was doing this, my colleague, Jatinder was anyway diligently working on the cover story of this issue, on cyber security challenges that are top up the mind for the CIOs, by talking to practitioners, experts, and going through Lords of research done recently. I urge you to go through his final list and analysis.

All I can say is that cyber security is increasingly resembling a competitive strategy game, with the stakes rising as the bar is raised. Interestingly, talking of AI, it is becoming a weapon at the hands of the attacker and a tool at the hands of the defenders - the cyber security managers.

While cyber security has consistently featured as a top risk, in the global risk report of the World Economic Forum, and the last few years, what is going to be different for the Indian enterprises in 2023 is the added responsibility of ensuring privacy of personal and non-personal data, as the privacy regulation comes in.

I would say the single most new challenge for Indian IT leaders in 2023 Is going to be ensuring data privacy. Hopefully, we will see a lot of deliberations around that in the next few months.

Well, just in case you are wondering what were the other two CIO priorities that ChatGPT pointed out, those were, talent management and working effectively with other business leaders to get the best value for the business leveraging IT.

I'm sure all of you can relate to all the four very well ■

CONTENT

NOVEMBER
DECEMBER 2022

COVER STORY

Cover Design by:
Shokeen Saifi

SILLY POINT

INSIGHT

5G

CIO&LEADER

www.cioandleader.com

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

EDITORIAL
Editorial Director - B2B Tech: **Shyamanuja Das**
Associate Editor - B2B Tech: **Jatinder Singh**
Assistant Manager - Content: **Dipanjan Mitra**

DESIGN
Sr. Art Directors: **Anil VK, Shokeen Saifi**
Sr. UI UX Designer: **Nikhil Wahal**
Sr. Visualiser: **NV Baiju**

SALES & MARKETING
Executive Director - B2B Tech:
Sachin Nandkishor Mhashilkar (+91 99203 48755)
Associate Director - Enterprise Technology:
Vandana Chauhan (+91 99589 84581)
Senior Manager - Community Development:
Neelam Adhangale (+91 93214 39304)

Regional Sales Managers
North: **Pratika Barua (+91 9999510523)**
West: **Vaibhav Kumar (+91 97176 74460)**
South: **Brijesh Kumar Singh (+91 98454 15137)**
Ad Co-ordination/Scheduling: **Kishan Singh**

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

Head - Digital & Event Operations: **Naveen Kumar**

OFFICE ADDRESS
9.9 Group Pvt. Ltd.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.)
121, Patparganj, Mayur Vihar, Phase - I
Near Mandir Masjid, Delhi-110091
Published, Printed and Owned by 9.9 Group Pvt. Ltd.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.)
Published and printed on their behalf by
Vikas Gupta. Published at 121, Patparganj,
Mayur Vihar, Phase - I, Near Mandir Masjid, Delhi-110091,
India. Printed at Tara Art Printers Pvt Ltd., A-46-47, Sector-5,
NOIDA (U.P.) 201301.

Editor: **Vikas Gupta**

9.9 GROUP

around the tech

KNOW THESE TOP TECH TRENDS

Global cloud security market size to grow from USD 48.57 billion in 2022 to USD 116.25 billion by 2028, at a CAGR of 15.7%.

RESEARCH REPORTS

IT leaders are prioritizing zero-trust

According to a research titled "The State of Zero Trust Transformation 2023" by Cloud Security company, Zscaler, over 90% of IT leaders that have begun their migration to the cloud have deployed, are implementing, or plan to implement a Zero Trust security architecture. It adds that IT leaders believe that Zero Trust is the best framework for protecting enterprise users, workloads, and IoT/OT environments in a highly distributed cloud and mobile-centric environment.

Global semiconductor revenue to decline

Global semiconductor revenue is projected to decline 3.6% in 2023, according to the latest forecast from Gartner, Inc. In 2022, the market is on pace to grow 4% and total $618 billion. Global semiconductor revenue is forecast to total $596 billion in 2023, down from the previous forecast of $623 billion. Gartner analysts foresee DRAM revenue to decrease 2.6% to reach $90.5 billion in 2022 and will further decline 18% in 2023, to total $74.2 billion.

Global private and public cloud market to grow by 18.81%

The Global Private and Public Cloud Market in the Financial Services Industry is expected to grow by $90175.21 mn during 2023-2027, accelerating at a CAGR of 18.81% during the forecast period, according to a study by Reportlinker.com. The market is driven by the growing demand for virtually unlimited storage and big data, the increased focus on cost optimization and scaling computation, and the high focus on sustainability using green IT.

Only 32% of employees believe their pay is fair

Less than one-third of employees feel they are paid fairly, while just 34% of employees believe their pay is equitable, according to a survey by Gartner, Inc. The Gartner survey of 3,523 employees in 2Q22 also found that employee who perceives their pay as inequitable have a 15% lower intent to stay with their employer and are 13% less engaged at work than employees who perceive their pay as equitable. According to the study, factors that erode organizational trust include poor culture and inclusivity, poor work-life harmonization, and unfair experiences.

Data analytics market size to be worth around USD 346.33 Bn by 2030

The data analytics market size accounted for USD 41.39 billion in 2022, according to Precedence Research, and will reach USD 346.33 Bn by 2030. According to the study, the introduction of ML and AI to provide individualized consumer experiences, the increased acceptance of social networking platforms, and the online shopping growth are the main factors propelling the market's expansion. Enterprises can improve crucial business processes, manage risks, accomplish goals, and activities by utilizing big data analytics and data driven intelligence.

India sees growing complaints of online financial fraud

India recorded 884863 complaints under the online financial fraud category from Jan 2021 to Nov 2022, according to National Crime Reporting Portal. In 2021, over 3500 people were arrested concerning cybercrime and more than 14000 cases were registered under this category, the government data reveals. 6,229, 10,395, and 14007 cases were registered under the category 'fraud for cybercrime' in 2019, 2020, and 2021.

Global cloud security market to grow at a CAGR of 15.7%

The global cloud security market size is expected to grow from USD 48.57 billion in 2022 to USD 116.25 billion by 2028, at a CAGR of 15.7% from 2022 to 2028, according to a new study by The Insight Partners.The cloud security market demand is driven by the rising number of cyberattacks, surging use of cloud-based solutions and managed security services, and increasing managed container services.

Organizations to focus on integrated T&E solutions

Through its subsidiary Amadeus Cytric Solutions, the travel technology solutions supplier Amadeus conducted the study, titled "Digital Transformation for Travel and Expense." The research firm contacted 525 top decision-makers from businesses with annual revenues between $100 million and $5 billion, as well as nearly 2,000 of their staff members and found that poor tool integration for managing travel and expenses, with manual procedures and security issues appearing as their main obstacles in seamless travel and expense reporting experience. According to the poll, only 52% of those surveyed globally were using fully integrated T&E systems, while 44% were only using ones that were only partially integrated.

M2M and IoT will be the most important use of Blockchain

Approximately one-third of technology executives believe that securing machine-to-machine interactions on the internet of things (IoT) will be the most important use of blockchain technology in 2023, according to "The Impact of Technology in 2023 and Beyond: an IEEE Global Survey." It says that compromised IoT devices, including medical devices and wearables, can alter data before it is sent to intended recipients, and the devices can also be compromised to illicitly send data to unauthorized recipients. Blockchain technologies can help make sure that the data that is being sent is valid and uncorrupted by any malicious party.

Ransomware attacks to grow in 2023

An increased risk of ransomware attacks in 2023 threatening to leak people's and businesses' valuable data if ransom demands aren't paid is anticipated, according to Avast, a global digital security player. Additionally, Avast researchers foresee optimization of social engineering used in scam attacks, taking advantage of economic hardships and energy crisis fears. The experts also expect increased malicious activity overall, as open-source malware becomes more accessible, and cybergangs recruit hacktivists to join their causes. Avast researchers further predict the already professionalized business of cybercrime will become more sophisticated. Additionally, Lockbit 3.0, a ransomware group, was the first ransomware gang to offer a bug bounty program in the summer, and others will likely follow suit.

Good leadership, strong tech usage are key to talent retention

The impact of the pandemic, the uncertain economic environment, and the burnout experienced by over half of Indian knowledge workers in the last year, have irrevocably changed what employees want from their leaders, according to new Slack research. The study, Leadership and the war for talent, based on a survey of over 2,000 Indian knowledge workers, found that stability, salary, and having a good manager are the top three factors for Indian knowledge workers when it comes to choosing the company they work for. being essential ingredients.

Appetite for tech deals will return in 2023

Faced with high inflation, an energy crisis, and falling consumer confidence, the biggest opportunity for tech companies in 2023 is to adopt an active mergers and acquisitions (M&A) strategy – according to an annual EY report, Top 10 opportunities for technology companies in 2023. As valuations come down, the appetite for deals is set to return next year. This is supported by a recent EY study, which finds that 72% of tech CEO respondents plan to pursue M&A in the next 12 months, compared with 59% of CEO respondents across all industries.

GOVERNMENT NEWS

RBI launches e-rupee pilot

The Reserve Bank of India has launched a pilot programme for the digital rupee aka e-rupee. Through specific partner banks, the digital money would initially be made available in a few large cities including Mumbai, New Delhi, Bengaluru, and Bhubaneswar. Both person-to-person and person-to-merchant transactions are compatible with it. Nine further cities – Ahmedabad, Gangtok, Guwahati, Hyderabad, Indore, Kochi, Lucknow, Patna, and Shimla will be added later. Four banks—State Bank of India, ICICI Bank, YES Bank, and IDFC First Bank—will participate in the test launch in the first phase. Later on, this pilot will include four more banks: Bank of Baroda, Union Bank of India, HDFC Bank, and Kotak Mahindra Bank.

Maharastra to use AI-powered cameras for crime prevention

The government of Maharastra will instal AI-enabled face recognition cameras to help reduce crime in Mumbai's streets. According to Deputy Chief Minister Devendra Fadnavis, the project is a part of the second stage of the Mumbai surveillance plan. Speaking on the eve of the 15th anniversary of the Mumbai terror tragedy was Minister Devendra Fadnavis. Within a year, the state government in Mumbai installed CCTVs as part of the first phase. The action was a part of carrying out a recommendation in a report that was submitted to the government following the terrorist incident of 26/11.

Karnatka rolls out AI-powered talent portal

An AI-powered portal that promises to offer complete services to assist job seekers in finding employment has been launched by Karnataka government. Aspirants can take a psychometric evaluation using the updated Karnataka Skill Connect Portal, which has 7,500 open positions right now. This can help them get better jobs.

J&K to launch a dedicated incubator for cybersecurity startups

The Jammu and Kashmir government plans to create a unique incubator for startups in the cybersecurity industry in order to encourage local businesses. In order to help new business owners, startups, and small and medium-sized enterprises (SMEs) already engaged in or planning to enter this industry, the Union Territory will also create a venture capital model (cybersecurity). The government notification also mentioned a suitable method for upholding transparency in the awarding of cybersecurity contracts. The government would implement personal identity assurance and other steps to prevent fraudulent practises and identify service users.

AIIMS experiences outages after cyberattack

The All India Institute of Medical Services, the premier public medical institution in India, was subject to a serious cyberattack that halted its servers. The attack exposed a large amount of the hospital's sensitive data as well as the computerised records of millions of patients, including VVIPs. The attack corrupted files and data on the hospital's primary and backup systems.Before online work could resume, the hospital had to take down its servers, network, and PCs for several days to clean up its systems and strengthen its cybersecurity. Numerous hospitals across the nation have been assessing their cybersecurity systems as a result of this event.

Digital government directory for citizens

Truecaller has launched an in-app digital government directory that will give easy contact access to thousands of verified government officials, law enforcement agencies, government institutes, hospitals, embassies, and helplines. Truecaller claims that the data came directly from the government and authorized government sources. Additionally, Truecaller has developed an easy procedure for any government body to exchange their verified contacts.

STARTUP NEWS

Shikhar Dhawan launches $75 Mn Sportstech fund

Shikhar Dhawan, an Indian cricketer, has launched a worldwide investment fund with a $75 million starting capital and a $25 million greenshoe option to invest in sports-tech firms. The fund targets deployment in Q1 2023-24. According to reports, the fund is a multi-stage, worldwide investment vehicle that primarily targets sports-related entrepreneurs. The fund would sign up athletes from various sports to represent them.

India registers over 18 lac EVs

The government has informed the Parliament that over 18 lakh electric vehicles (EVs) are currently registered in India, with the biggest numbers of registrations occurring in Uttar Pradesh, Delhi, and Maharashtra. Union Road Transport and Highways Minister Nitin Gadkari stated that Uttar Pradesh has the most registered vehicles in this segment with over 4.1 Lakh EVs in a written response to the Rajya Sabha. Delhi comes in second with more than 1.8 Lakh registered EVs.

Uolo Raises $22.5 Mn Funding

Uolo, an edtech startup, has raised $22.5 million in a Series A funding round led by UAE-based venture capital firm Winter Capital. Blume Ventures, an existing investor, and Morphosis Venture Capital, based in Dubai, have also participated in the funding round. Uolo was founded in 2013 to provide learning programs in coding and English speaking.

Ola withdraws infotainment service

Ola, an Indian ride-hailing startup, has discontinued its 'Ola Play' infotainment service in select ride segments. The in-car infotainment service, which was launched in 2016, was a popular feature in several of its sedan cars across cities such as Delhi, Bengaluru, Hyderabad, and more, allowing users to access music, videos, and other such services while on the move. Customers would be charged a small fee for cabs equipped with infotainment systems.

Samsung invites startups to collaborate to scale, build tech-solutions

Samsung, a manufacturer of consumer electronics, is inviting startups to work with it on technologies related to the Government of India's Digital India stack, which includes, among other things, UPI, Digilocker, Open Network for Digital Commerce (ONDC), Open Credit Enablement Network (OCEN), and Unified Health Interface (UHI). According to the company, the entrepreneurs will collaborate with Samsung's R&D facilities and commercial departments in India on projects in the areas of wallet, health, and fitness where the company's ecosystem will be incorporated into the goods and services. The company will also explore funding support to some startups to help them further scale their solutions.

Number of unicorns in India dropped to 85

According to data gathered by Finbold, the number of unicorns (startups with a $1 billion valuation and beyond) in India decreased from more than 100 to 85 during the current economic crisis. US leads the unicorn rankings with 705 unicorns, followed by China with 243 unicorns. The United Kingdom ranks fourth with 56, while Germany ranks fifth with 36 unicorns.

MediBuddy completes its merger with DocsApp

MediBuddy has completed the merger with the online consultation platform, DocsApp. With this merger, all operations of DocsApp will end, and all subscribers to DocsApp will be helped make the transition to the new consolidated organization. The two businesses, which had been operating under the parent firm Phasorz Technologies up until this point, announced their merger in 2020.

KreditBee raises $80 Mn

KreditBee, a lending tech business based in Bengaluru, has raised $80 million from current investors Premji Invest, Motilal Oswal Alternates, NewQuest Capital Partners, and Mirae Asset Ventures as part of its continuing series D investment round. Additionally, Mitsubishi UFJ Financial Group (MUFG) Bank took part in the round. With the money, KreditBee intends to expand the range of products it offers to include secured loans, house loans, and credit lines as well as services like insurance and credit score reporting.

CIO MOVEMENTS

BALAJI RAJAGOPALAN **joins State Bank of India as Chief Technology Officer (CTO)**

Balaji Rajagopalan has formerly worked at ICICI as the bank technology group head for the corporate centre, capital markets, and intelligent automation.

Landmark Group ropes in VIKRAM IDNANI **as President -CIO**

Vikram Idnani has been named president and chief information officer (CIO) for Landmark Group's India business, a leading retail and hospitality group in the Middle East, Africa, and India.

RAVI PICHAN **joins RBL Bank as CIO**

Ravi Pichan will be responsible of leading the Bank's technology strategy and will also assist in the creation of a technology innovation hub to encourage a culture of continuous innovation within the Bank.

ASHOK JADE **joins Kirloskar Brothers as Global CIO**

Ashok joins from Spark Minda where he served as Group CIO. Ashok was earlier associated with Shalimar Paints, Videocon Industries Ltd and Tekcare India Private Limited.

NEXT100 Winner AMIT GHODEKAR **promoted to SVP-Information Security at Axis Bank**

Before this, Amit was working as the Vice President - Information Security at the same company.

VIKRAM GUPTA **promoted as Senior Director, Technology at Snapdeal**

Vikram Gupta has been promoted to Senior Director of Technology at Snapdeal. Before this, he was Director of Technology at the same company.

Licious appoints AJIT NARAYANAN **as Chief Product and Technology Officer (CPTO)**

D2C meat and seafood firm Licious in Bengaluru appoints Ajit Narayanan as its CPTO. Prior to Licious, Ajit was the CTPO and founding member of MFine, a health-tech business.

Nykaa appoints RAJESH UPPALAPATI **as CTO**

With over 20 years of rich experience in creating world-class products, platforms, and services for both large corporations and start-ups, Rajesh joins Nykaa following a successful tenure at Intuit.

APARNA KUMAR **joins State Bank of India as CIO**

She joins from HSBC where she served as CIO, India. Aparna was earlier associated with HDFC Bank, Capgemini and I Flex Solutions Ltd.

Around The Tech

INDUSTRY MOVEMENTS

SANDHYA DEVANATHAN NAMED as Vice President of Meta India

Meta, the parent company of Facebook, WhatsApp and Instagram, has appointed Sandhya Devanathan as the Vice President and Head of Meta India. Sandhya comes with more than two decades of experience. Sandhya joined Meta (then known as Facebook) in 2016. She held positions as the business director for Vietnam and Singapore's country managing director before being promoted to vice-president of gaming for Meta APAC, where she presently works.

Zoomcar appoints NAVEEN GUPTA as VP and India Head

Naveen Gupta has been appointed as the company's vice president and country head for India by car-sharing startup Zoomcar. In his new position, Gupta will be in charge of the organization's growth, operations, and customer experience in India. Gupta has more than 11 years of experience in the auto and online retail sectors. He previously worked for Hero MotoCorp, redBus, Swiggy, and Cars24. He has an MBA from the Indian Institute of Foreign Trade.

AMIT CHOUDHARY is the new COO of Wipro

Amit Choudhary has been appointed as the chief operational officer and a member of the Wipro executive board by the technology services and consulting firm Wipro Limited. Choudhary will oversee organisational operational effectiveness and responsible for promoting sustainable growth.

NXP Semiconductors appoints HITESH GARG as the new India Country Manager

Hitesh Garg has been named as NXP Semiconductors' new Country Manager for India. Garg, who has worked with NXP for more than 14 years, succeeds Sanjay Gupta, who served as the company's previous national leader.

ANGAN GUHA is Birlasoft's new CEO-MD

Technology services and consulting company, Birlasoft has appointed Angan Guha as its new CEO-MD. A former senior executive of Wipro, Guha will also join CK Birla group's entity Birlasoft board as a full-time director.

DEEPA MADHAVAN is Genesys's new India Head

Cloud customer experience and contact centre solutions provider Genesys announced the appointment of Deepa Madhavan as the India-Country Head. Deepa, in her new role would continue the development of Genesys cloud technologies and engagement of teams across all functions in Genesys India. Prior taking up the new role, Deepa was serving PayPal.

Cybersecurity in 2023:

What's keeping tech honchos up at night?

The top cybersecurity challenges are driven by the organization's ever-growing hybrid workforce culture and digital footprint.

BY JATINDER SINGH

The COVID-19 pandemic has exposed the unpreparedness of many conventional organizations to respond to widespread disruptions and security risks. Nearly 30% of those firms that face such assaults are expected to suffer severe financial losses in addition to business interruption and reputational harm.

With more people turning online for work, service consumption, and leisure, cybercriminals have an unprecedented opportunity to leverage sophisticated tools to launch their exploits and target key infrastructure for information theft.

According to EY Global Information Security Survey (GISS) 2021, the COVID-19 crisis has had a devastating and disproportionate impact on cybersecurity. Through a global survey of more than 1,000 senior cybersecurity leaders, the research finds CISOs and security leaders grappling with inadequate budgets, struggling with regulatory fragmentation, and failing to find common ground with the functions that need them the most. Enterprise security has become increasingly exposed as a result of the growth of work from anywhere, linked devices, and multi-cloud systems, which has also led to an increase in security breaches.

IBM estimates that the average cost of a data breach in India increased by around 6.6% from 16.5 crores in 2021 to 17.6 crores in 2022. In our cover story for this issue, we will examine the key challenges and significant areas of attention for tech leaders in 2023 concerning cybersecurity.

A RISE IN RANSOMWARE ATTACKS

Cybercriminals utilize ransomware, a sort of software, to profit financially. It is distributed similarly to how all malware infiltrates victim systems. According to Palo Alto Networks' Unit 42 Ransomware Threat Report 2022, the average ransom demand in instances they handled in 2021 rose 144% over 2020. Additionally, there was an 85% rise in the number of victims whose names and other information were made public on the "leak sites" on the dark web that ransomware gangs employ to blackmail their victims. These and other widespread extortion techniques are a sign of what the ransomware threat landscape will look like in the future.

"Ransomware and its impact pose a huge challenge as it will cause disruptions to work and business challenges. It is important to have the right controls in the right place to ensure protection against Ransomware, Malware. The burden of this is relatively significant given the data at stake and the financial impact of paying the ransom."

JASPREET SINGH
Clients and Markets Leader - Advisory Services, Grant Thornton

CERT-In noted that India witnessed double the ransomware attacks in 2021 compared to 2020, leading to more organizations paying ransoms. Ransomware gangs are increasingly using many extortion strategies to coerce the target organization into paying the demanded ransom, which is a growing trend.

A malware assault on several Central Depository Services (India) Limited's computers occurred in November of this year, causing settlement operations to be delayed. In another incident, the All India Institute of Medical Sciences (AIIMS), India's foremost medical institution, experienced a large cyberattack on its networks, which was reportedly a ransomware attack. It compromised every file stored on the hospital's primary and backup systems in addition to interfering with routine medical operations, which had an impact on thousands of patients.

These are only a few of the numerous incidents that afflicted IT decision-makers in 2022 as they dealt with their cybersecurity initiatives.

Organizations will be more susceptible to assault in 2023 as hybrid working continues to rule most of the world. Industry experts predict that in the coming year, ransomware attacks would concentrate more on damaging data than encrypting it. Organizations need to become comfortable talking about cyber risks in the same way they talk about market risks and establish workable plans, according to KPMG. This can involve applying a "trust but verify" philosophy when it comes to the security tools your company uses and taking into account new business services that offer software assurance and continuously

Digital trust extremely important for 9 out of 10 organizations

- 42% of consumers have stopped doing business with a company after losing trust in that company's digital security
- If companies do not manage the digital trust, 88% of their customers would consider switching
- 91% of consumers in APAC are concerned about cyber threats, more than anywhere else in the world
- 99% of enterprises believe it is possible that their customers would switch to a competitor if they lost trust in the enterprise's digital security.

Source: DigiCert Survey

monitor your technological environment.

To manage a larger range of threats, risk and security professionals will need to think beyond traditional approaches to security monitoring, detection, and response. Most IT leaders place a greater emphasis on developing robust automation and security intelligence layers to protect against such ransomware concerns. In 2023, more emphasis will be placed on creating a solid data backup strategy to make sure that, in the event of a system attack, the crucial data is not destroyed.

In addition, to protect the company IT infrastructure, the IT teams should hold regular education and training sessions to teach staff the best practises, such as how to spot phishing, create strong passwords, and utilise separate devices for personal and business use.

EXPANSION OF IoT

As we get closer to the information-driven 5G era, data is the glue that holds enterprises together, whether it's driving exceptional user experiences, increasing services, or anticipating customer needs. Across 2023, the ubiquity of connectivity, which will also enable frictionless data collection and transfer, will drive the widespread deployment of IoT sensors in sectors and industries across verticals. To increase production and efficiency, these connected devices are anticipated to see significant growth in the manufacturing sector.

Because there are so many of these devices, it is difficult for IT decision-makers to assess their multi-layered and end-to-end security requirements. These devices are also becoming more and more likely access sites for hackers. According to the 2020 Unit 42 IoT Threat Report, by Palo Alto Networks, 57% of IoT devices are vulnerable to medium- or high-severity attacks, making IoT the low-hanging fruit for attackers.

The IT decision-makers contend that there is no one-size-fits-all approach to enhancing an organization's cybersecurity when it comes to IoT and that to prevent these devices from becoming easy targets for cybercriminals, solid policies must be in place even during the deployment phase.

"There is a thin line of demarcation between IT and IoT and this is where security gets dropped as IoT exposes the enterprise and significantly increases vulnerability to attacks."

MAITREY MODHA
Head - APAC
Technology & Quality,
CNH Industrial India

AI-POWERED ATTACKS

As AI has gained prominence, it has helped businesses by successfully streamlining their processes and automating tedious jobs. The technology has also been leveraged by enterprises to enhance their customer service and provide real-time support. It is also equally effective in enabling enterprises to identify possible threats in advance.

According to an IBM study, implementing AI and automation in security can help firms cut the entire expenses of a data breach by saving more than 14 weeks in threat detection and response times. But these days, technology is also being utilized destructively, and cyber criminals frequently use it to further illegal ends. The worry that cybercriminals may abuse AI is not new. The cybercrime industry, however, has never had the financial resources to construct tools or attract extraordinary AI expertise, which may put large businesses in a precarious position as they have all the resources and skill sets necessary to allay such fears.

The security company McAffe claims that soon, employees will be able to create AI-generated content in a matter of minutes since AI-driven content production tools are becoming more widely accessible to

the general public, customers at home, and employees. The same goes for desktop publishing, photo editing, and low-cost photorealistic home printers, which will provide sophisticated outputs previously only possible with specialized knowledge.

The 2023 threat predictions report adds that "improvements in desktop publishing and consumer printing also brought benefits to criminals by enabling better counterfeiting and more realistic image alteration."

Although the industry hasn't yet seen widespread AI-powered ransomware attacks because they would require highly skilled cybercriminals, many believe it's only a matter of time because cybercrime is developing into a professional industry and soon they may start hiring AI experts for illegal activities.

Experts predict that these technologies will help scammers and propagandists, including cybercriminals and others attempting to fool the public, progress their tradecraft with more effective and realistic results.

The use of AI-enabled tools by hackers to contaminate data and influence decision-making algorithms could modify the intended behavior of AI/ML tools used by enterprises, which might pose a big problem for IT decision-makers in 2023. It will be a challenging task for tech leaders in to create effective defenses against AI-powered attacks. Strong AI-governance initiatives must be put in place by IT leaders to combat and prevent the risks to privacy and potential exploitation of data.

According to Gartner, there is no monitoring available to evaluate the impact on privacy because a substantial portion of the AI used by enterprises today is embedded into larger systems. These embedded AI capabilities are used to analyse consumer sentiment, follow employee activity, and create "smart" goods that adapt as they are used. Furthermore, judgments made years from now will be impacted by the data supplied into these learning models today.

"Once AI regulation becomes more established, it will be nearly impossible to untangle toxic data ingested in the absence of an AI governance program. IT leaders will be left having to rip out systems wholesale, at great expense to their organizations and to their standing," notes Nader Henein, VP Analyst at Gartner in a report titled, Gartner identifies top five trends in privacy through 2024.

Cybersecurity talent

- 87% of organizations implemented a training program to increase cyber awareness. However, 52% of leaders continue to believe their employees still lack the necessary knowledge
- 67% agree that the shortage of qualified cybersecurity candidates creates additional risks for their organizations
- 60% struggle to recruit cybersecurity talent
- 52% struggle to retain qualified people

Source: Fortinet 2022 Cybersecurity Skills Gap Global Research Report

"We cannot leave security at the mercy of the coder or security team, it has to be embedded in processes and systems. We have to ensure every level is secure — from the IDE from where the coder is coding it to the different gate-ways from where the whole appli-cation pipeline flows."

RAMAN PILLAI
Director IT
VerSe Innovation

NEW AND ADVANCED SOFTWARE SUPPLY CHAIN THREATS

When the SolarWinds hack was originally announced a few years ago, the supply chain attacks were heavily highlighted. According to industry analysts, supply networks will be more vulnerable in 2023 as we draw closer to that year. It is anticipated that hackers may leverage contemporary techniques and resources to target weaknesses at specific points in the software supply chain.

According to Kaspersky Security Bulletin (KSB), an annual project lead by Kaspersky experts, the main problem for 2023 will be supply-chain stability and cybersecurity. "Supply-chain will become more of a sweet spot for targeted ransomware and state-sponsored espionage campaigns,"it says.

According to ReversingLabs, the reality of software supply chain attacks hasn't been lost on developers and those working for software firms. To assess organizations' levels of awareness about supply chain risks, ReversingLabs commissioned a survey of 307 executives, as well as technology and security professionals at software publishers. According to the Dimensional Research poll,

there are growing worries about software supply chain threats and the dangers that come with an increased reliance on open source and third-party libraries.

CYBERSECURITY TALENT GAP

Cybersecurity skill scarcity has long been a problem for tech industry leaders, and this problem is expected to continue through 2023. Despite an expanding talent pool, attracting and keeping qualified cybersecurity professionals has become a top challenge for tech leaders. Cloud security specialists, Security Operations (SOC) analysts, Security administrators, Security architects, DevSecOps specialists, incident response specialists, and Network architects are among the main roles that enterprises are looking to fill.

The risk of data breaches and hackers has increased as a result of the new and emerging technologies such as AI and ML. Because of the extraordinary size and pace of the attacks, businesses must constantly assess their risk management plans, and this need strong availability of talent.

Across the world, 80% of firms experienced one or more breaches that they could link to a deficiency in cybersecurity knowledge and/or skills, according to the Fortinet 2022 Cybersecurity Skills Gap Global Research Report. According to the report, 64% of firms had breaches last year that cost them money in lost sales or fines. Organizations reported breaches that cost them more than $1 million in a startling 38% of cases.

Despite having an estimated 4.7 million experts, the cybersecurity workforce still faces a global shortage of 3.4 million people, according to ISC's 2022 Cybersecurity Workforce Study. Its findings show that an additional 65% growth in the global cybersecurity workforce is required before all firm personnel requirements would be satisfied.

NEW REGULATIONS AND DATA PRIVACY

Data privacy compliance and local rules have recently emerged as a major issue impacting critical business decisions as firms strive to advance digitally. The amount of data being produced today is enormous, and there are numerous complex laws and regulations in place around the world to deal with it, including the General Data Protection Regulation, China's Cybersecurity Law, and India's proposed Digital Personal Data Protection (DPDP) law, among many others.

Although experts concur that these laws are necessary for a nation's and its residents' security, they can also result in conflicting priorities, which could somewhat jeopardise an organization's security. According to Gartner, 75% of the world's population will have their personal data protected by contemporary privacy laws by the end of 2024.

Many firms will recognise the necessity to begin their privacy programme efforts now as privacy regulation activities spread across dozens of jurisdictions over the course of the next two years. In fact, Gartner forecasts that by 2024, large enterprises would spend

"To enhance defence and safeguard critical information, organisations must stay one step ahead. Besides deploying strong monitoring tools and policies, strengthening security awareness, behaviours, and culture is extremely crucial and a top priority for organizations."

MAHESH KORIA
SVP & Head - BIU,
Axis Bank

Trends, and challenges that incident responders experience

- Organizations that are essential to the global economy, supply chains, and the movement of goods have become prime targets for disruptive attacks
- 77% of Cybersecurity Incident Responders (IR) in India say they have experienced extreme or considerable mental strain as a result of responding to a major cybersecurity incident
- Ransomware has exacerbated the psychological demands of IR for 94% of respondents in India
- The high demands of cybersecurity engagements also affect incident responders' personal lives, with 68% of respondents in India experiencing stress or anxiety in their daily lives. Insomnia, burnout, and impact on social life or relationships followed as effects respondents cited.

Source: The global survey of over 1,100 cybersecurity incident responders in 10 markets, conducted by Morning Consult and sponsored by IBM Security.

more than $2.5 million annually on privacy. Technology leaders may find it difficult to balance maintaining compliance with making sure they are abiding by all laws in the nations in which they do business.

NATION-STATE CYBER THREATS

Organizations in every industry must be prepared to deal with nation-state cyber threats in 2023. In a scenario, where cloud is enabling businesses and organizations to connect across the globe, threat actors and cybercriminals are extensively looking to attack government and enterprise infrastructure that are far outside of their historical boundaries. These assaults use highly effective methods to undermine public confidence, steal technological capabilities and sway opinion.

The proportion of nation-state assaults that target crucial infrastructure that Microsoft has identified has jumped from 20% to 40% since last year. This spike was primarily brought on by Russia's desire to damage the infrastructure of Ukraine and its persistent espionage campaigns against its allies, mainly the United States. The Microsoft research states that "in addition, many attacks are also coming from China, which is propelled by its ability to uncover and create "zero-day vulnerabilities" - particular unpatched gaps in software not previously known to the security community."

In addition, coordinated and destructive cyberattacks have also been noticed from Iran and North Korea.

Industry experts say it's crucial for businesses and technology leaders to find the approach that best fits their needs rather of concentrating on the tried-and-true method. Enhancing protection mechanisms absolutely requires paying attention to fundamentals and culture transformation. If sufficient multi-factor authentications, pertinent policies, and automated threat detection technologies are not enabled, cybercriminals can simply attack susceptible environments in a hybrid configuration where hundreds and thousands of connected devices are present in an organization's ecosystem.

According to industry experts, new technologies like artificial intelligence (AI) are being used to battle cybersecurity risks. AI aids in the detection of new assaults or intrusions as well as the development of security protocols. IoT and 5G together usher in a new era of technological advancement and hazards. A multitude of assaults that could be introduced by the 5G architecture must be screened using advanced hardware and software. A similar amount of attention would be paid to training, process improvements, and developing in-house cybercrime talent in 2023 ■

Key technologies in focus to mitigate cybersecurity risks

Zero-trust architecture (ZTA): Zero-trust capabilities are being adopted with considerable attention to the threat and risk environment they really deal with as well as their business goals.

Behavioral analytics: Analytics tools that not only orchestrate preventative and incident response actions but also offer risk-based authentication and authorization.

Homomorphic encryption: By enabling users to work with encrypted data without first decrypting it, this technology makes it safer for internal collaborators and other parties to access big data volumes. Additionally, it aids businesses in complying with stricter data protection regulations.

Defensive AI and machine learning: To detect and fix non compliant systems, businesses will need to scale up their AI and ML capabilities. They also need to optimise tech stacks and workflows to make the best use of the available resources.

Automation for risk assessments: Automated settings, software upgrades, and patching for low-risk assets. A strong priority area will be risk assessments, segmentations, and identification of further vulnerabilities by utilising automated capabilities.

Source: Cybersecurity trends: Looking over the horizon, McKinsey

"There is definitely a shortage of talent as few people have expertise in new technologies and come with a mindset to solve real problems. Even if we find them, retaining them is a different ball game altogether."

SATYA KALIKI
CTO
Infra.Market

COLUMN

By Dr. Prashun Dutta

CIO and Ubiquitous Presence of Technology

Former CIO, project management expert and author Dr. Prashun Dutta, in the second article in a series on key changes in the CIO role with changing environmental factors, takes up the role of CIOs in an era IT's role moves from making an impact at the function/project level to doing that at the entire organization level.

The present scenario is, obviously, in sharp contrast to the situation half a century ago and the main point of difference is the extent of usage of technology in business organizations. Role of computers and communication then was limited to a small set of functions and activities. A few departments used computers to record and maintain various books and extract reports after transactions were completed and records updated. In contrast today we have no part of any organization untouched by automation technologies. We transact, report, analyze using these technologies we also interact amongst ourselves, with customers, partners, and even various regulatory authorities on digitalized platforms. Software helps us in our decision-making process through analytics, machine learning, accessing data anywhere in the world; technologies like IoT, Edge computing help us "see" what is going on in the opaquest of places, it assists with our security; visualizing possible outcomes through intelligent simulation, and several other critical activities. In short, every single aspect of our functioning is majorly informed by use of technology. Convergence of several basic technologies (Mechanical, Electrical, etc) with microprocessor-based instrumentation and controls along with continuous improvement in the latter have gained IT a ubiquitous presence and a prima donna status, in business organizations.

This, as can be assessed, is a major change that significantly impacts the responsibilities and specifically the way of working of the CIO. Let me elaborate on this point further. By virtue of its all-round presence IT is in a unique position to integrate working of an organization. A common experience in organizations is

often associated with the difficulty of achieving reasonable alignment in working of its different limbs. While this is true for mid-size organizations the problem is far more acute in large ones, as may be expected. Achieving such unified functioning is a major objective of any complex entity and would form the foundation for the next step of integrating with the environmental eco-system. Integrating with partners, vendors, and governmental & regulatory limbs. Studies have unequivocally shown that when any logistics system interconnects its constituents the efficacy of the overall system improves substantially. The IT function, by intelligent design and execution, could play a pivotal role in integrating the entity and that could be indeed be a game changer.

The question that arises at this juncture in what way will this impact responsibilities and activities of a CIO? Well now the minimum unit for consideration is the entire organization and not any part of it. Earlier the CIO or the IT function would suggest IT enablement for a particular part of a department's function, for instance payroll or inventory control or any such application and that would be discussed for taking forward. Now however, any such proposal for introducing use of technology would necessarily have to be for the organization as a whole. The starting point for discussions on IT functions and activities will have to commence with the organization-wide road map. This road map will derive, partially from the strategic plan pursued by the organization and equally from present day technological innovations. The road map will comprise a full depiction of all applications and technological initiatives that are envisaged for the organization; an aspirational picture to be pursued sedulously. It is this that would need to be approved by the top management and all initiatives should be presented within this framework.

Such a road map, if presented with its concomitant benefits, would achieve a buy-in of leaders in the organization. It would help in developing a vision of how the organization will function in future and associated technology that shall be used to achieve this. A road map shall elucidate how technology will be utilized to augment functioning of the organization and the manner in which different functions will be integrated to benefit managers and end users. It would stress on enhanced productivity, more informed decision-making, real-time monitoring of critical parameters and so on, that would substantially enhance efficacy and, as mentioned earlier, will be a real game changer. Such an action will provide a high level of comfort and confidence to the top management; they will be able to understand that the CIO has a plan that is effectively aligned to that of the organization. This acceptance can be further augmented by getting an external expert to talk to members of the top management which would build sufficient confidence in the plan. Additionally, if the top management so desires, this plan can be vetted by a 'subject matter expert' who may be external to the organization, and his verdict sought. Additionally, the plan needs to contain sequence of implementation, and estimates associated timelines and costs along with assumptions on which these are based. Such a document, discussed threadbare with senior officials in business and top management of the organization, would be a source of confidence for the top management.

In conclusion, technology had started off as a minor contributor to organizational functioning but now has become a major player with clear potential to be a game changer, if used properly. The approach of earlier CIOs was to propose individual projects covering a part of a function or even a data rich process. However, with extensive broad basing of technology in the functioning of today's organization a holistic approach covering the entire organization and integration of its part must be the focus now. New projects will necessarily have to be within the overall master plan. One question that begs answer is how the CIO will prepare such a master plan. We will dwell on this question in the next article ■

SILLY POINT

By Akash Jain

Spotlight: Spatial Computing

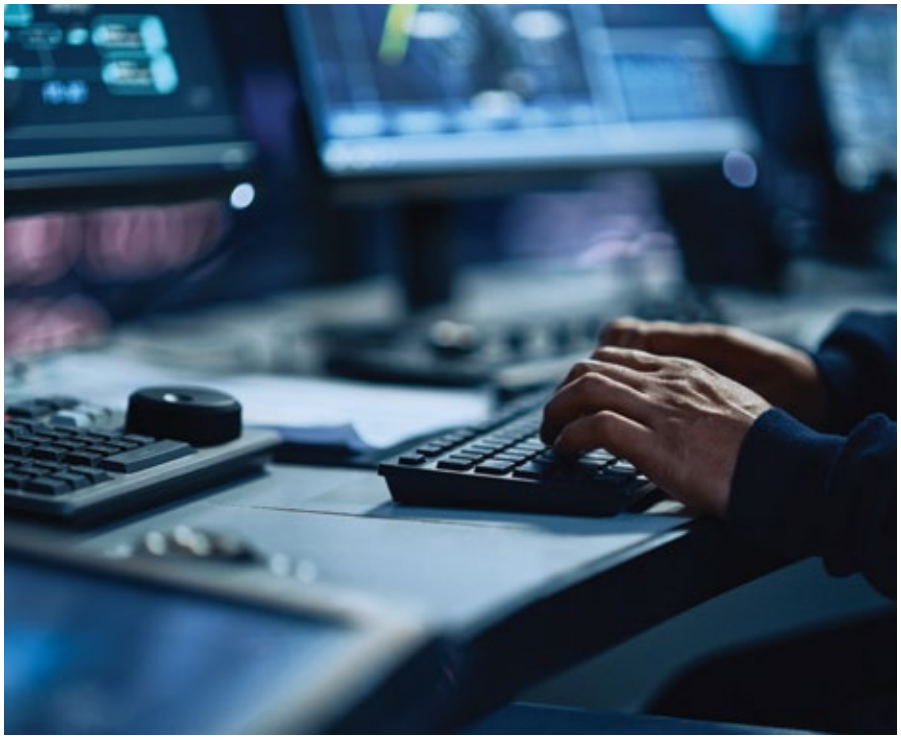
This is the 6th column of the series called Navigator MasterClass, wherein we will find our way through the myths and realities of one Bleeding Edge technology each month; in terms of where it truly stands at the time of writing, and its business applications- implemented, being attempted, or speculative. This month's topic is Spatial Computing (SC). A technology that has hundreds of definitions, almost like the elephant and the blind men. So, let's trace its origin in very brief.

Simon Greenworld coined the term in his 2003 MIT Graduate Thesis paper, defining it as "human interaction with a machine in which the machine retains and manipulates references to real objects and spaces". Let us look at a more precise technical definition, presented by a group of researchers at the 2007 Seminar on Computing Media and Language for Space-Oriented Computation: "a field of research in Computer Science where space is not an abstract notion, but a first order effect that has to be optimized".

In basic terms, SC extends digital world into the real one, by using light, sounds, images, trackers, sensors, and haptic devices. It does so by using a combination of Virtual Reality, Augmented Reality, Mixed Reality, Edge Computing and Digital Twins platforms. The implementation manifests itself by using physical actions (head and body movements, gestures, speech, eye focus) as inputs for interactive digital systems, and physical spaces as output base for video, audio, and haptics.

A potential industrial application is a single operator operating, monitoring, and managing multiple machines SIMULTANEOUSLY, a la an orchestra conductor. Not surprisingly, Gaming has been

The author managed large IT organizations for global players like MasterCard and Reliance, as well as lean IT organizations for startups, with experience in financial and retail technologies



the pioneering user of this technology. It is now being experimented with, in HR (training), Product Development, and Virtual Tours in tourism and real estate.

As can be expected, the usual players are betting billions on SC: Microsoft, Alphabet, Facebook (Metaverse, anyone!), Apple, Amazon, Tesla, and so on. There are also start-up disruptors like Magic Leap which has raised billions of dollars in funding (including during the recent pandemic) in its 12 years of existence and is developing technology to superimposes 3D computer-generated imagery over real world objects; it does so by projecting a digital light field into the user's eye. Its enterprise platform, Magic Leap 2 releases on September 30, 2022; it promises to be an immersive device with optics with up to 70° diagonal FOV. Let us now look at three products being developed by Microsoft. The first one is Dreamwalker; it turns the user's physical walk into a VR experience. Say someone wants to walk to the grocery store and experience a walk through the Mughal Gardens in Delhi. The walk will look and feel like what you wanted it to be, with the turns and obstacle avoidance as needed in the real-world walk. This is real time manipulation of VR: insertion of obstacles in the VR walk, so that you physically move around the obstacles (like a person walking towards you).

The second is Mise-Unseen; it senses the eyes to find out where the user's gaze and attention is focused, and changes objects in the other parts of the VR world without the user realizing it. The third stunning platform is Capstan Crunch; it uses haptic controllers to create physical pressures and sensations in a virtual world. An example would be the user catching a ball in mid-air. Let's now look at where the world of SC is heading. McKinsey is convinced that retailers will soon need to become "experience designers". This will increasingly become easier with Quantum Computing become available on a mass scale (just waiting for one technical breakthrough, that could happen any day); making SC's mass adoption easier.

Gartner on the other hand believes that SC is one of the six expected primary uses of Metaverse (the other five being Gaming, Digital Humans, Virtual Spaces, Shared Experiences, and Tokenized Assets (NFTs)). They do go on to predict that these will become reality by 2030, because the platforms are still in "innovation" stage.

MIT projects three trends that will emerge: dynamic workplace redesign, co-working transformation, and ubiquitous computing. All of these are implementations of SC. They go on to ask a very interesting question to highlight the role of SC: "Previously, new digital communication technologies caused some theorists to predict "the death of distance" - liberating us from the office space. Today's technology does allow global and instantaneous communication, but most of us still commute to offices for work every day. Why?"

The second thing they project is that People and Machines will become even closer partners in innovation. An example they quote is Alphabet's DeepMind that developed a software called AlphaZero in 2017. This program was ONLY taught the rules of chess. After just one day of playing itself, AlphaZero crushed the current leading software (which was unbeaten by any human); and chess masters learnt new tricks and moves from AlphaZero. It is not hard to imagine the level such partnership will reach when you add SC to this.

We end with addressing the elephant in the room. What are the chances of misuse and abuse with SC becoming mainstream. Is it like the nuclear fission technology which started with good intentions, and ended up creating the atom bomb too? Certainly, registry-based distributed computing platforms like blockchain will help; but humans will need some more work on who teaches the chess rules to SC platforms ■

INSIGHT

The New Pillars Of Modern Security: Workloads, Identities, And Data

Security teams need to consider workloads (endpoint and cloud), identities (user and machine), and data as the epicenter of enterprise security risk.

By Amol Kulkarni

People, processes, and technology have long been the core pillars dictating how cybersecurity programs are managed, and with good reason: organizations need well-trained talent on their staff, trusted processes in place to prevent breaches and respond should they occur, and the latest security technologies to detect and block malicious activity. This layered approach to security has protected organizations for many years. However, this alone won't keep organizations safe as adversaries continue to sharpen their techniques .

While the "people, process, and technology" tenet remains critical, IT and security teams must think about how these three pillars span three important domains that organizations should prioritize in their defensive strategies. Security teams need to consider workloads (endpoint and cloud), identities (user and machine), and data as the epicenter of enterprise security risk and the new "three-legged stool" informing their approach.

Workloads: endpoint and cloud

Adversaries view the cloud as an opportunity to pursue intellectual property theft, data extortion, and ransomware campaigns, among other goals. Common cloud attack vectors include vulnerability exploitation, credential theft, cloud service provider abuse, use of cloud services for malware hosting and command-and-control (C2), and exploitation of misconfigured image containers.

Of course, cloud workloads aren't the only ones that need protection. Security teams must protect endpoints as well, and these have different risk profiles and threat exposure. When setting their sights on endpoints, adversaries continue to demonstrate how they have moved beyond malware. Rather, they have been observed using legitimate credentials and built-in tools - an approach known as "living off the land" - to evade detection by legacy antivirus products.

As organizations grow and add more endpoints, cloud workloads, and containers, as well as new tools to protect them all, security can quickly become complicated. Security teams should enable runtime protection, obtain real-time visibility and eliminate configuration errors as part of their best practices

Identities: user and machine

Most breaches are now identity-driven (80% to be exact) - a stat that should motivate security teams to carefully think about their identity protection strategies.

Credential-based intrusions against cloud environments are among the more common vectors used in both cybercrime and targeted attacks. Cybercriminals often host fake authentication pages to collect legitimate credentials for popular cloud services, then use them to attempt to access victim accounts. They just need one valid set of credentials to log in as an employee - assuming additional security measures don't get in their way.

As part of their defense strategy, organizations should ensure full deployment of multi-factor authentication (MFA), especially for privileged accounts; disable legacy authentication protocols that don't support MFA; and track and control privileges and credentials for both users and cloud service administrators.

Data: the importance of data protection

Ultimately, adversaries target data. As organizations think about the future of data protection, they should consider how workloads (endpoint and cloud), identities (user and machine) and data are interconnected - and how data changes based on how these assets interact. Identities are authenticated via endpoints, while code repositories, cloud workloads and applications are accessed through the endpoint. Data flows from asset to asset, and it exists across devices and across cloud environments.

It's a big job to protect all of this data, and it looks slightly different for every organization. There are many steps that security teams can take to help protect the data ■ **Enable cloud workload protection:** Protecting workloads demands visibility and discovery of each workload and container events, while securing the full cloud-native stack on any cloud across workloads, containers and serverless applications.

- **Protect all identities:** Adversaries use stolen credentials to bypass legacy defenses and disguise themselves as legitimate users. Security team require a strong focus on identity to protect organizations from modern threats.
- **Know what to protect:** Organizations must have an enterprise-wide understanding of their data assets. Unified visibility of assets, configurations and activity can help detect misconfigurations, vulnerabilities and data security threats, while also providing insights and guided remediation.

Now more than ever, organizations must think about security across every part of the business. As the attack surface grows amid the increased adoption of cloud computing and remote work, enterprise security must encompass all workloads, identities, and data. Every CISO should make these three layers top of mind ■

— The author is chief product and engineering officer, CrowdStrike

Debunking The Most Popular Cyber Security Myths In India

Here are six common cyber security myths analyzed and debunked for the benefit of business leaders.

By Diwakar Dayal

Gone are the days when cyber security was merely a technical or niche issue to be dealt with by some small department in the basement. Today, cyber security is highly complex as it has to work with new operational technologies, evolving business needs, and an expanding attack surface. The Board of Directors needs to have clarity on the impact of cyber security risks while making strategic business decisions. They should also have an understanding of what to ask when a breach occurs to avoid catastrophic consequences.

Much of the information available on cyber security and cyber risk is buried in sales and marketing jargon, which is unique and subjective as perceived and conveyed by one vendor or another. This is often aimed at a technical audience and not always relevant to the decision-makers. Here are six common cyber security myths analyzed and debunked for the benefit of business leaders.

Myth 1: Cyber Security is only necessary for some businesses

It is a common belief among business leaders that not all organizations require cyber security. They assume there is a requirement only for technology companies, businesses that store sensitive customer data, or have a legal requirement to meet, and companies of a certain size or value. This is, however, not true. Cyber security is critical for all organizations, irrespective of which industry vertical they belong to. Impacted organizations will experience financial loss, customer churn, and brand damage among other negative consequences. India recorded 36.29 lakh cyber security incidents from 2019 till June this year. As per information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total of 3,94,499, 11,58,208, 14,02,809 and 6,74,021 cyber security incidents were observed during 2019, 2020, 2021 and 2022 (upto June) respectively.

Myth 2: Security Software is all that the organization needs to stay safe

Many pinpoint tools such as SIEM, SOAR, Firewalls, Anti-Virus, and others in the cyber security defense arsenal have proven to be insufficient to keep attacks at bay. The modern, remote working models provide more freedom to employees than before as they can install software and gain access to the organization's assets from anywhere. Although the effort of protecting assets from attacks may start with acquiring the appropriate tools, it does not end there. This is because the threat landscape is continuously evolving and the organization's defense capabilities must keep pace too. It is critical to weave in cyber resilience with the overall strategic vision of the organization.

Myth 3: Software vulnerabilities are not an issue for the Board

Every software an organization leverages can also introduce vulnerabilities that can increase the company's attack surface and make it easier for cyber attackers to penetrate the corporate network. Unfortunately, the operating system itself is among the most likely source of vulnerabilities in the software stack. In 2020, Microsoft confirmed 1,220 new vulnerabilities impacting their products, a 60% increase from the previous year. 807 of the vulnerabilities were associated with Windows 10, with 107 of those related to code execution, 105 to overflows, 99 to gaining information, and 74 to gaining privileges. In 2021, 836 new vulnerabilities were confirmed, 455 of which impact Windows 10 and 107 allow malicious code execution. Boards have to understand that the patch management done by the IT team will not protect them from the security risk presented by the operating system itself. Organizations must explore partnering with security-first companies that provide a holistic approach to security and not rely on the OS vendor either to patch everything or to provide security add-ons to plug the gaps.

Myth 4: There is no need to worry about supply chain attacks

Sometimes even if an organization ensures to safeguard its software, there is a possibility of other service providers unknowingly facilitating a way into the network. The recent SolarWinds supply chain attack where the attackers were able to compromise organizations through SolarWinds software update, and the Kaseya incident in which attackers targeted Kaseya VSA servers - commonly used by MSPs and IT management firms to infect downstream customers with ransomware.

Such attacks are highly lucrative for threat actors because compromising one weak link, enables access to a complete portfolio of customers using that software. The C-Suite has to take a strategic decision of ensuring there is maximal protection against digital supply chain attacks.

The Board's strategy should include, deploying of the right security solution, the developing of an Incident Response plan, ensuring application integrity policies only allow authorized apps to run, and driving a cyber security-centric culture.

Although employees are a key part of the organization's cyber security strategy, one cannot expect them to be experts at it.

Myth 5: Organizations cannot do anything about cyber security threats

Several measures can be taken by businesses to protect themselves from the most likely attacks and reduce the risk of being targeted by cybercriminals. In the majority of cases, threat actors preying on businesses are financially-motivated and are looking for easy wins. Like spotting the weakest animal in the herd, organizations that cannot safeguard themselves will be quickly picked off by cyber predators. Organizations should implement a comprehensive cyber security plan that should include several layers of security to protect themselves from most attacks.

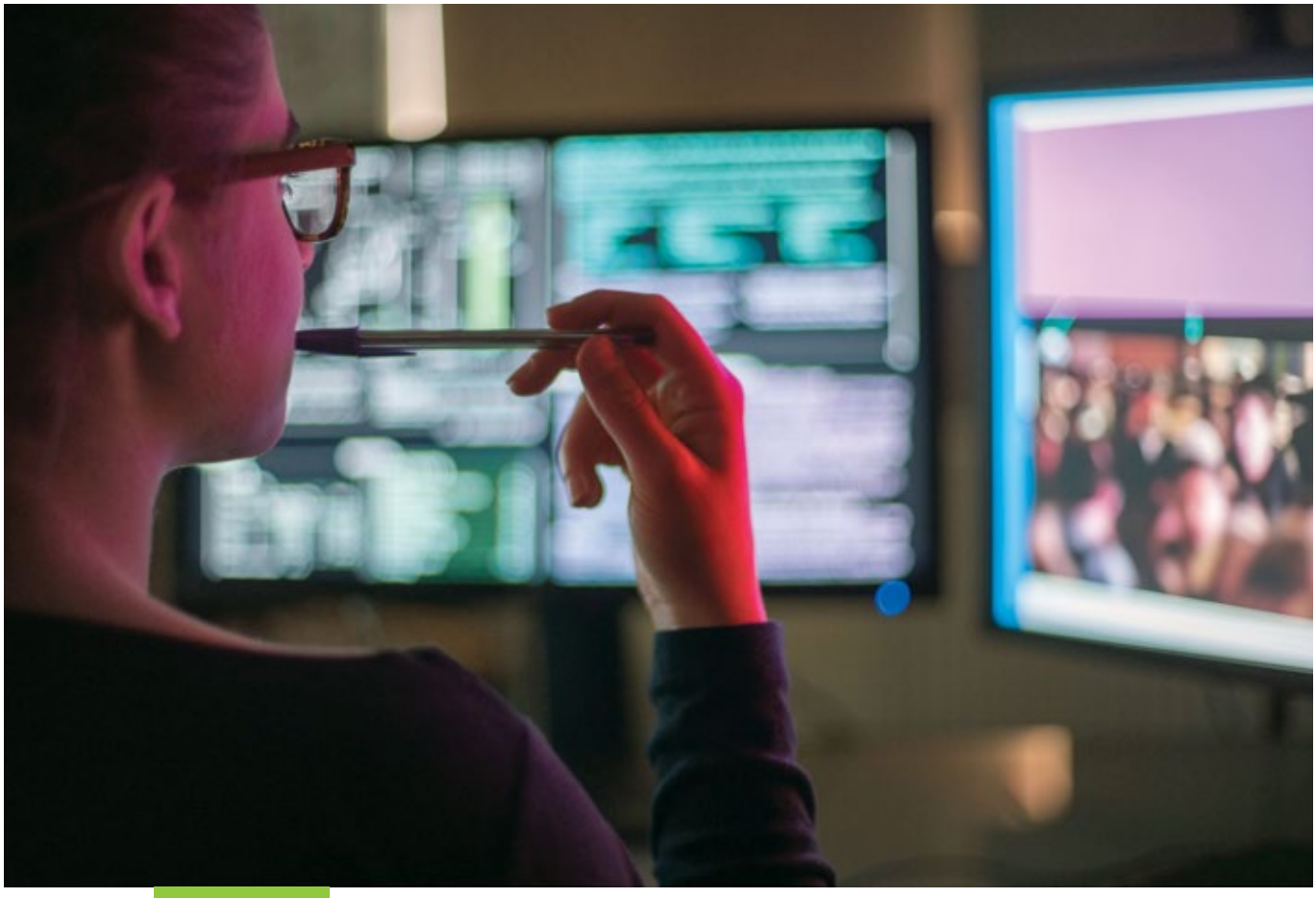
Myth 6: It is impossible to train employees to be cyber secure

Although employees are a key part of the organization's cyber security strategy, one cannot expect them to be experts at it. It is the responsibility of the organization to provide employees with appropriate training and resources. This should include awareness programs on the kinds of threats the business may face, simple steps on how to identify issues like phishing emails or unusual requests, and clear steps for reporting suspicious activity. Employees are to be considered as an aid to the organization's cyber defenses.

Conclusion

After debunking cybersecurity myths, the C-Suite will be better equipped to effectively manage risks. In today's threat landscape, it is important that cyber security is approached as a strategic initiative by the company's leadership, involving all key departments. It should be carefully planned and executed by the top management, so that it may be cascaded down to the rest of the workforce. The risk for the business is too high if cyber security planning isn't done in a holistic way ■

—The author is Managing Director & Country Manager for SentinelOne, India & SAARC



Cybersecurity In The Education Sector

Higher education has long been a target for cyberattacks due to research programs with potentially valuable data.

By Debasish Mukherjee

According to a report* Education and research were the most targeted sectors in India, with an average of 1,605 weekly attacks, an increase of 75 percent from previous years. Data also shows that there has been a 20 per cent increase in cyber threats to the global education sector in the first three months of 2022 when compared to the corresponding period of 2021.

Many may not know this but higher education has long been a target for cyberattacks due to research programs with potentially valuable data. These institutions are also often considered an easy target due to a large number of users and entry points on college campuses. But attacks are on the rise – and they are not relegated to higher education.

In May, a breach of education software provider Illuminate Education exposed data of over 1 million current and former students across New York State, and K-12 schools and school districts have increasingly become targets for attack in part because of the shift to remote learning. In fact, in 2021, the education industry saw a 152% spike in ransomware attacks and an average of 22% were targeted by malware attacks each month, according to recent data from SonicWall.

As the education industry faces the same impacts of rising cybersecurity threats, educational institutions must take the following steps to invest in their security:

Adopt a security mindset

There are two security mindsets. One philosophy that has become popular over the past several years assumes bad actors will get in no matter what, using network monitoring to identify and mitigate threats. Another involves guarding the perimeter to prevent bad actors from gaining access in the first place.

In this instance, both have their merits – guard the perimeter to make cybercriminals' jobs more difficult and monitor the network in case those protections aren't enough. This is especially important for education institutions given the vast number of devices on their networks.

Guard the perimeter

One of the most effective ways to guard the perimeter is to adopt a Zero Trust framework – requiring continuous authentication and validation of all users before allowing access to data and applications. This can be daunting for an educational institution with many users and small IT teams - but it's essential to ensure data remains secure and in the right hands.

Additionally, ensure to arm users with the right tools and knowledge to protect themselves. According to Verizon's 2021 Data Breach Investigations Report, 85% of breaches involve a human element, so humans – the users – are an important first line of defense and a critical component of your cybersecurity strategy. One way to set users up for success is to implement stronger password policies and multi-factor authentication to add a layer of protection. This is particularly important since so many educational tools run off the cloud and can be accessed nearly anywhere with just a password.

It is also important to train users – including students, educators, and staff – to watch out for signs of cyberattack. One of the most common attacks they should be aware of is Business Email Compromise (BEC), a type of social engineering scam deployed to get users to hand over fraudulent payments, login credentials, and other sensitive information.

Secure and monitor networks & Wi-Fi

Wi-Fi powers learning for college campuses and K-12 schools alike, and it also serves as an easy gateway for malicious attacks. One way to improve Wi-Fi security is through a content filtering service that compares requested sites against databases to deny access to potentially harmful websites.

Implementing a network monitoring solution is crucial to identify security threats and performance issues and ensure all systems are operating properly and securely. Equally important is network segmentation – dividing networks into smaller parts – so that cybercriminals can't take down your entire network in the event of an attack.

Prepare an incident response and disaster recovery plan

Incident response and disaster recovery planning is crucial for education providers. One of the most important steps to prepare for a breach is backing up critical data. This ensures that the mission-critical data is available even in the event of a breach - without paying a costly ransom. A proper plan should also inform educators and other users of what to do and who to go to in the event of a suspected cybersecurity incident so that IT and security teams can respond quickly and minimize damage. If 2021 was any indication, the threats facing the education industry aren't slowing down any time soon, with never-before-seen malware and other threats continuing to rise. But if education providers prepare, they can greatly improve their chances against cyber criminals ■

—The author is Regional Sales APJ at SonicWall Inc.

New Threat Trends -"More Is More" The Mantra Cybercriminals Live By

From RaaS to new attacks on non-traditional targets like edge devices and virtual cities, the growing volume and variety of increasingly sophisticated cyberthreats will surely keep security teams on their toes in 2023 and beyond.

By Vishak Raman

While "less is more" being the strategy of CISOs behind consolidating networks and security, "more is more" seems to be the mantra cybercriminals continue to live by. As we look at our threat predictions for 2023 and beyond, there is "more" at every turn. Cybercrime will converge with advanced persistent threat methods and cybercriminals are finding ways to weaponize new technologies at scale to enable more disruption and destruction.

New Threat Trends in 2023 and Beyond

It's not surprising that cyber adversaries will continue to rely on tried-and-true attack tactics, particularly those that are easy to execute and help them achieve a quick payday. However, FortiGuard Labs predicts that several distinct new attack trends will emerge in 2023. Here's a glimpse of several attack developments we'll be watching for in the next year:

- **The Explosive Growth of CaaS:** Given cybercriminals' success with RaaS, we predict that a growing number of additional attack vectors will be made available as a service through the dark web. In addition to the sale of ransomware and other Malware-as-a-Service offerings, we'll also start to see new a-la-carte criminal solutions.
- **Money Laundering Meets Machine Learning:** We also expect that money laundering will get a boost from automation. Setting up money mule recruitment campaigns has historically been a time-consuming process. We anticipate that cybercriminals will start using machine learning (ML) for recruitment targeting, helping them to identify potential mules better while reducing the time it takes to find these recruits. Over the longer term, we expect that Money Laundering-as-a-Service (LaaS) is also on the horizon, which could quickly become part of the growing CaaS portfolio.
- **Deep Web Destinations Welcome a Wave Cybercrime:** And while newer online destinations like virtual cities that take advantage of augmented reality (AR), virtual reality (VR), and mixed reality (MR) technologies open a world of possibilities for users, they also open the door to an unprecedented increase in cybercrime. From virtual goods and assets that can easily be stolen to potential biometric hacking, we expect this attack surface will result in a new wave of cybercrime.
- **Wipers Become Rampant:** Malware that may have been developed and deployed by nation-state actors could be picked up and re-used by criminal groups and used throughout the CaaS model. Given its broader availability combined with the right exploit, wiper malware could cause massive destruction in a short period of time given the organized nature of cybercrime today.

Protecting Your Organization Against the Evolving Threat Landscape.

Understanding the lifecycle of an attack can go a long way in helping you protect your networks—the MITRE ATT&CK framework is an excellent resource. Implementing network segmentation is also critical in protecting your organization against cybercriminals. Segmentation improves security by preventing attacks from spreading across a network and infiltrating unprotected devices. In the event of an attack, segmentation also ensures that malware can't spread into your other systems.

Yet the most important action you can take to enhance your organization's security posture is to adopt a broad, integrated, and automated cybersecurity mesh platform. Cybersecurity defenses have traditionally been deployed one solution at a time, usually in response to an emerging challenge. But a collection of point solutions simply doesn't work in today's growing threat landscape. Consolidation and integration into a single cybersecurity platform is crucial. Using an inline sandbox service is a good starting point to protect against sophisticated ransomware and wiper malware threats. It allows real-time protection against evolving attacks because it can ensure only benign files will be delivered to endpoints if integrated with a cybersecurity platform.

Implement network segmentation and micro segmentation

Network segmentation offers many benefits for businesses. Segmentation improves security by preventing attacks from spreading across a network and infiltrating unprotected devices. In the event of an attack, segmentation also ensures that malware can't spread into other enterprise systems. Micro segmentation is a network security technique that enables security architects to further segment an environment for lateral visibility of all assets in the same broadcast domain. Granularity is achieved by logically dividing the network environment into distinct security segments down to the individual workload level. Because policies are applied to individual workloads, micro segmentation offers enhanced resistance to attacks. And if a breach does occur, it limits a hacker's ability to move among compromised applications ■

—The author is Vice President of Sales, India, SAARC and Southeast Asia at Fortinet

Best Practices To Secure Your Organisation

Break through the silo mentality and teach everyone in a company to be aware, alert and pro-active, so that the cyber cleaning process is constant.

By Rick Vanover

In tech industries critical messages need to be repeated often. Sometimes they can be complicated, so we reach for analogies to make messaging, particularly around problem-solving, more relatable. Discussing cyber security and the rise of ransomware attacks is more critical than ever because the problem is more prevalent than it's ever been. Finding effective ways to drive the messages home so that true change can rapidly take place is a constantly inventive process.

Emerging from two years of pandemic-related restrictions and resulting impacts on business, the concept of hygiene is immediately relevant to IT. When we were under attack from a virus, we wore masks, we washed our hands, were careful around others and defended ourselves and those most dear to us. We can apply these analogies directly to the topic of cybersecurity, which needs its own practices of hygiene.

October was Cyber Security Month and in Australia we witnessed an alarming spike in ransomware attacks on large corporations, maliciously affecting millions of citizens whose personal data was compromised. That is the publicly known tip of a huge iceberg wreaking havoc all year and involving many organisations across the 16 countries surveyed in Veeam's 2022 Ransomware Trends Report. The report presents a confronting picture of the effectiveness and pervasiveness of bad actors. It shows that 80 per cent of attackers seek out mainstream systems with known vulnerabilities, and that nearly 50 per cent of data centre servers, remote offices and cloud-hosted servers were targeted and encrypted in 2021. The figures will be higher for 2022 and we will see multi-layer, end-to-end attacks.

The threatscape is evolving

Cyberattacks are getting more sophisticated. Longer dwell time, less obvious pattern recognition capability with intermittent encryption, all make an attack more difficult to detect. With the ability of attackers to branch out horizontally, erasing data at will, a ransomware payment within deadline won't have prevented rapid data theft, deletion, or both.

If your house contains valuable possessions, you are unlikely to display them by an open door under spotlights. You are going to lock the doors and get motion detector lights. If you have an alarm, you are going to set it, and you will teach everyone in the family how to set that alarm before they go out or go to bed. The home security analogy is another way to consider cyber security. Reduce the threat of inviting thieves to your home. Reduce the threat of having your company's data stolen or wiped.

Best practices to protect a business

Every individual in a business is part of the security solution. Hire backwards in the pipeline, find young hungry graduates who can be trained from the start in these practices. Break through the silo mentality and teach everyone in a company to be aware, alert and pro-active, so that the cyber cleaning process is constant and when a breach occurs, nobody is paralysed. Much of the threat vector can be eliminated with simple, mandatory steps, teaching all staff to focus on the big picture while paying attention to the small details. Don't click on that link. Practice patch management. Change the password. Update the firmware. Train users on Phish. Set up multifactor authentication, not just for remote access, but for all critical applications. The simplest way to exfiltrate data is to use the applications already in place that do not cost extra. They are the human components of everyday digital cleaning and essential before even looking at backup processes.

Backup is the last line of defence

The house is clean and in order, but theft can and will still happen. Secure backup is your last line of defence against ransomware. You can only recover what you backed up. Ransomware has democratised data theft, since targeted data only needs to have enough value to the victims, so they are convinced to pay ransom to recover that data. This model of ransomware has been successful despite increased investment in defensive security technologies. Look for a software-defined approach with no lock into proprietary hardware, working with your company's existing architecture and operating both on-premises and in the cloud. Ensure it is a portable data system that can be moved securely at a moment's notice. When there is an attack, the data can be brought back, but not to where it was stolen from. The nuance is how that data is retrieved and how quickly it is secured in a new destination.

Good digital hygiene will always be a company-wide responsibility. There is no single person, regardless of role, who is not a participant in the security response team for your organisation. Your team is your defence force. And your data service provider is an essential weapon in your armoury. Working together, the battle can be won ■

—The author is Senior Director Product Strategy, Veeam and Dave Russell, Vice President Enterprise Strategy, Veeam

Compliance Requirements For Startups In India

Top 6 compliance requirements every startup should meet

By Manoj Shastrula

India owns the third-largest startup ecosystem in the world, valued at $340.79 billion. With a YoY growth rate of 15% since 2018, the country is home to 75,000 startups and 107 unicorns as of 2022. More than 80 startups register with the government daily, spreading across 56 sectors and 635 districts.

The Indian government has introduced several business-friendly initiatives like the 'Make in India' campaign and the 'Startup India' program to support the world's fastest-growing startup ecosystem. Emerging startups can earn recognition by registering online and avail of incentives and economic benefits such as tax exemption to boost their businesses. However, the Department for Promotion of Industry and Internal Trade (DPIIT) will only acknowledge entrepreneurship if it complies with the legal and statutory regulations of the land. Businesses not adhering to the laws may get hefty penalties and even imprisonment for entrepreneurs responsible for operational activities. Moreover, non-compliance can deface the company's public image, repel the customer base with the anticipation of fraudulence, negatively influence employee morale, and impair the overall business performance.

Here are the top 6 compliance requirements every startup should meet to avoid criminal charges and promote company growth.

Business-specific statutory framework

India identifies business entities as one of the four primary structures—One-person Company, Private Limited Company, Partnership Firm, or Limited Liability Partnership. Accordingly, the enterprise should abide by the regulations defined in the Companies Act 2013, Partnership Act 1932, or Limited Liability Partnership Act 2008.

Startups desiring to register with the government must decide on their operational format and conform to the corresponding rules. They must incorporate legal compliance from inception and adhere to the registration procedure inextricably. Professional assistance can ease the process, and mentorship from industry experts may help establish a legitimate internal culture like minimum wages, maternity leaves, employee protection, and worker satisfaction and well-being.

Company mandates and licenses

Some entrepreneurs require industry-specific licenses that do not apply to other businesses. For example, a food joint or restaurant needs Food Safety License and must satisfy the Prevention of Food Adulteration Law that a footwear business shouldn't. Similarly, registered companies must follow mandatory compliances regarding board meetings, annual general meetings, auditor appointments, director's reports, maintaining financial statements and books of accounts, and filling in relevant forms that establish them to be lawful. Transparency in business operations and law-binding governance build credibility among stakeholders and ensure increased efficiency.

Taxation compliances

Startups registering with the startup India program enjoy tax exemptions and financial benefits to promote their growth. Initially, they can avail of exemptions on long-term capital gains, investments above their fair market value, tax holidays, and 100% tax rebates on their profits for three years out of the first ten years of their incorporation. Filling out Income Tax Returns, Tax Audit Reports, TDS Returns, and Assessments of Tax Liability under the Income Tax Act 1961 align the company with the country's economic regulations. Moreover, the business should submit monthly, quarterly, and annual GST returns under the GST Act 2017 to remain functional.

Intellectual Property Rights (IPR) compliances

Startups rely on strategic innovation, creativity, and unique business models to penetrate the market with valuable products, services, or processes. Their assets may secure Copyrights, Trademarks, or Patents to prevent illicit use. The Startups Intellectual Property Protection (SIPP) scheme launched by the Government of India enables entrepreneurs to file applications for IPR through registered coordinators by paying appropriate statutory fees. The initiative led by National Research Development Corporation provides general advice on preserving IPR, disposes of IP applications for original designs and products, appears at hearings on behalf of startups, and contests oppo-

In the digital era, every startup thrives online and executes consumer interaction virtually. Cloud-based business operations or the internal digital infrastructure of a company may suffer from security concerns, cyber attacks, and data breaches.

sition by breaching parties if necessary.

Compliances for employee protection

India's business framework involves Acts and regulations like Employee Provident Fund Scheme 1952, Maternity Benefit Act 1961, the Minimum Wages Act 1948, the Contract Labour (Regulation & Abolition) Act 1970, Trade Union Act 1926, etc., to safeguard labours against exploitative practices and facilitate employee well-being. Startups must protect workers against workplace abuses, sexual harassment, corruption, layoffs, and financial malpractices to comply with the legalities. Moreover, they must document contractual obligations between the parties in legally-binding formats to establish the lawful functioning of the company and its stakeholders.

Cybersecurity compliances

In the digital era, every startup thrives online and executes consumer interaction virtually. Cloud-based business operations or the internal digital infrastructure of a company may suffer from security concerns, cyber attacks, and data breaches. The COVID-19 pandemic-related remote working witnessed a 75% spike in daily cybercrime, with 55% data leakage, 51% phishing emails, and 35% ransomware attacks. Small and medium-sized businesses (SMBs) are increasingly vulnerable to cyberterrorism due to their laxity in adopting security policies. Breaches of Personally Identifiable Information (PII), financial information, or Protected Health Information (PHI) can cost the organisation's reputation and financial loss.

Moreover, poor cybersecurity governance and mishandling of consumer databases can be penalised under the Consumer Protection Act 2019 and the Information Technology Act 2000. Startups that fail to comply with cybersecurity regulations and lack consumer protection policies encounter hefty financial penalties from authorities. For example, HIPAA charges $100 to $50,000 per violation of security norms, while Payment Card Industry Data Security Standard (PCI-DSS) penalises the organisation with monthly fines between $5,000 to $100,000.

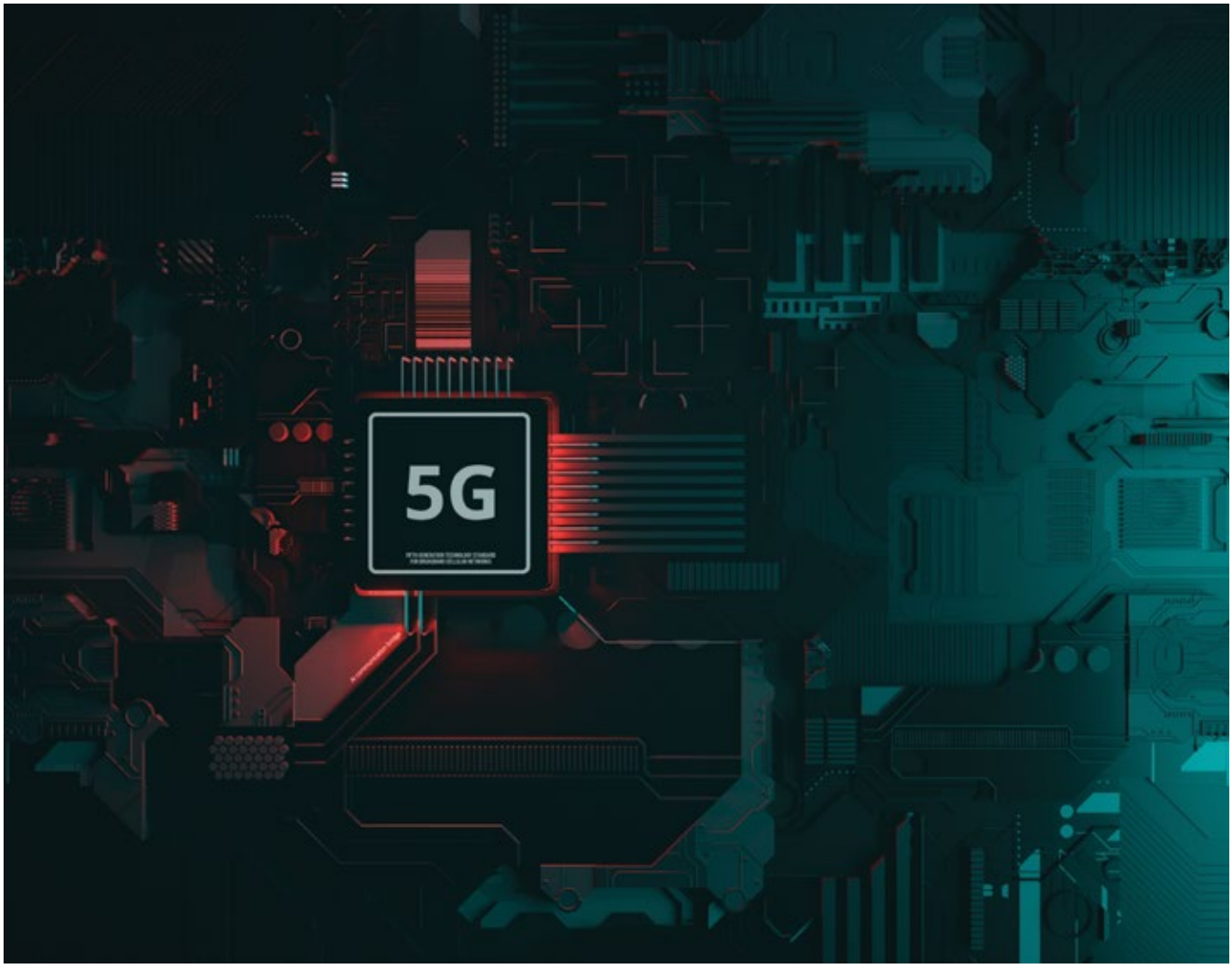
Thus, businesses must deploy a robust digital security framework to preserve sensitive information's confidentiality, Integrity, and Availability (CIA). A comprehensive cybersecurity foundation identifies tech support fraud, theft attempts, social engineering attacks, malware, and other sophisticated threats. It promotes operational efficiency, prevents fines and penalties, protects confidential data, and helps gain consumer trust.

Integrated data protection platforms that automatically collect thousands of data points of processes, policies, people, assets, and vendors in a unified interface provide complete control over the company's security program and increased visibility to compliance status. They help businesses identify potential vulnerabilities and combat sophisticated cyber threats with zero hassle and delays. Most importantly, these platforms automate compliance with data security standards of SOC2, ISO 27001, PCI-DSS, HIPAA, NYDFS, GDPR, etc., and protect intellectual properties with systematic risk governance approaches.

Final words

Startups making blunders complying with statutory requirements end up crashing with heavy financial punishment. Though the regulations can be overwhelming, over 14,000 entrepreneurs earned recognition in fiscal 2022 with investments up to $3.5 billion across 130 deals. Abiding company mandates, taxation and licensing compliances, IPR protection, employee well-being, and cybersecurity governance help startups to facilitate seamless performance, enjoy government benefits, and gain consumer trust and confidence ■

—The author is CEO & Founder, SOCLY.io



5G: A catalyst for enterprise transformation

The emergence of Industry 4.0, the development of smart infrastructure, and network slicing are some of the major factors driving the growth.

Earlier this year, India announced the launch of 5G. As of now, the country's top two telecom service providers, Reliance Jio and Bharti Airtel, have begun to provide 5G services in select cities, with 5G services expected to be available in all cities by the end of 2023.

According to the industry experts, more than providing speedy connectivity to consumers, 5G has been designed to help enterprises transform their data-driven ecosystems by increasing their ability to control various services and generate real-time insights for exceptional user experiences.

Next-generation wireless networks, for example, will alter how cities manage public transportation, medical professionals provide telehealth services, manufacturing enterprises automate their factory operations, and broadcasters deliver real-time content. It can strengthen supply chains, provide round-the-clock visibility, and predict real-time outcomes in seconds using efficient data analysis.

New opportunities

Experts predict that 5G technology will accelerate digital transformation across industries, including healthcare, education, transportation, agriculture, and public safety. According to Gartner, 5G specifications provide a new way of assembling and operating technology through cloud-native and service-based architecture, enabling CIOs and other tech leaders to break away from previous generations of technologies to shape operational platforms.

Gartner adds that the technology is an opportunity for CIOs to develop infrastructure and services operations as platforms to meet diverse needs of various lines of business.

According to Markets and Markets, the 5G enterprises market is expected to reach $10.9 billion by 2027, growing at a CAGR of 31.8% between 2021 and 2027. The emergence of Industry 4.0, the development of smart infrastructure, and the delivery of differentiated 5G services using network slicing techniques are some of the major factors driving the growth of 5G.

According to the study, the main challenge is the requirement for high-spending carriers to establish 5G infrastructure. Low latency connectivity with uRLLC will drive growth, as will increasing demand for private networks from various enterprises and government organisations for mission critical applications.

According to Gartner, 5G will enable CIOs to develop infrastructure and services operations as platforms to meet diverse needs of various lines of business.

As intelligence migrates to software, applications migrate to open platforms, and computing migrates to the edge, there is an opportunity to engineer platform and application components, innovate and deliver differentiated, contextual solutions, and identify new efficiencies. Many 'waiting' use cases, such as digital processing of medical scans, micro finance, and asset management opportunities, will become viable as a result. This will open new opportunities in industries, businesses, and ports, among other places.

Smart strategies needed

The increasing number of connected devices would necessitate significant changes in enterprise data centre strategy. Increased server pressure can put enormous strain on data centres and the number of services available.

Overall, a key point of discussion would be the compute strategy with the speed that 5G will generate or the traffic that 5G will generate. Data traffic at the edge can strain the capacity of the access network.

According to recent discussions we've had with some well-known technology professionals, 5G is more than just another voice and data transmission technology. It is a chance to unleash previously unheard-of economic growth by providing digital enablement to businesses across industries, geographical regions, and remote places. Young talent has the chance to assume the initiative in advancing engineering-led innovation.

In the following pages, we will present some key CIO perspectives on 5G and how the technology will impact enterprises ■

Success of 5G wireless services hinges on strategic planning

PANKAJ CHOPRA
SVP & Head UNOC
Bharti Airtel

There's been a lot of buzz about 5G lately, and it is understandable. The next generation of wireless technology holds tremendous potential to transform the way we live and work. However, to reap the advantages it offers — such as ultra-latency and extreme throughput — the entire ecosystem needs to work as a unit and execute well to deliver the relevant use cases. Equally critical is the privacy and security of connections, devices, and applications that run on the 5G networks. A robust cybersecurity foundation is crucial from the network user standpoint and a national security perspective.

One needs to understand that the amount of investment for 5G is high. The use cases currently are not yielding relevant results. There will be new use cases and revenue streams for mining, manufacturing, retail, and education industries as we progress.

In terms of deployment, 5G first needs to integrate with the already established 4G LTE networks. Some of the first rollouts of 5G networks are likely to be on non-standalone (NSA) tracks that focus on integration with existing 4G networks to provide superior data bandwidth and connectivity. In NSA, the existing 4G LTE network assets leveraged for everything, excluding the 5G data plane. The selection of 5G deployment options – whether NSA or standalone (SA) – by service providers will depend on their investment appetite, business goals, and the individual use cases of their networks.

"It's essential to create right strategies around network rollout, customer requirements, privacy and security and ROI."

5G networks need comprehensive network testing on parameters, such as latency, throughput, and availability. However, there are limited trial licenses currently. As we look forward to an ultra-fast connected future, it's essential to define the right strategy from the network rollout perspective and the customer standpoint. The ecosystem of all the innovators – related to devices, applications, ISVs – will have to come on one platform to lead the charge to develop and unlock the true value of 5G ■

5G will amplify the adoption of Edge to drive innovative use cases

ROCHAK KAPUR
EVP & Head - Enterprise Products & Business Operations,
Vi Business

The fifth-generation wireless technology is designed to be a multi-service network and primarily brings three key capabilities: enhanced mobile broadband, ultra-reliable low latency, and massive Internet of Things (IoT) opportunities.

The above capabilities can be translated into business use cases that require edge computing and network slicing not just on the core but also on the radio network to give hybrid networks to enterprises.

This emanates from having multiple network slices and each slice running for different enterprise requirements locally but also at the same time giving the capability of a public network to the organization through the remaining set of slices.

Many of our customers currently with a private network, whether 4G LTE or 5G shortly, are looking to develop strong capabilities in the space of automation, Industry 4.0, robotics, smart factory management, and high payload requirements such as security and surveillance.

In addition, 5G will be instrumental in pushing more and more compute and capability to the edge. While it's the use case in an enterprise that will drive the decision about edge location, for the success of any high bandwidth capabilities scenarios across enterprises, the telco edge and enterprise edge would be of equal importance.

As a country, we have got a very imaginative and innovative workforce. There is no dearth of use cases. We need to build market-specific use cases which have business viability leveraging the agility and flexibility of the future-ready networks. 5G holds tremendous potential to impact societies, lives, and businesses positively ■

"Combining 5G and edge computing will enable enterprises to get real-time network visibility and drive new data-driven use cases hitherto not possible."

Not just another voice and data wave!

VIVEK DIXIT
Head-EPC, Reliance Jio Infocomm

The 5G revolution will transform how we work, collaborate, and connect to create new offerings for business (B2B) and consumer (B2C) markets.

5G is not just another voice and data wave! It's something that can transform the whole ecosystem. For Communication Service Providers (CSP), this technology transformation opens up new avenues in B2B business while enhancing value for B2C business, a vast but challenging opportunity. IoT would be the first gainer for enterprises. 5G will be a massive leap for the manufacturing sector, which will leverage it for IoT applications.

The true advantage of 5G, a cloud-native technology, would be the standalone (SA) mode functioning, powered with network slicing and end-to-end network orchestration and automation. Use cases specific to the Indian ecosystem would be the key to exploiting its potential.

The intersection and integration of 4G and 5G will be challenging. 4G has taken a massive leap, so 5G adoption and frictionless integration with 4G would be crucial in evolving the mobility network. The industry needs to find various combinations and technology approaches to deliver the best-always connected experience.

"A well-defined roadmap, policies, and infrastructure development efforts are needed to create a winning 5G ecosystem."

The co-existence of private LTE and 5G is another area enterprises will be focusing on to get ultra-low latency and incredibly high bandwidth connections, supporting numerous AI and IoT-based applications. The process of service continuity needs to be streamlined.

Developing a winning 5G ecosystem would require stakeholders to work together to identify relevant use cases. The government has a significant role in taking 5G technology benefits to the rural area. A collaborative approach can ensure that agriculture, education, medical, and healthcare sectors immensely benefit and leverage 5G for resource availability even in the remotest areas ■

5G will be a game changer for video experiences

MANISH PAINULY
Director (Digital Transformation, Cloud & Web Scaling), Viacom18

While 5G is yet to be launched in India, there is a tremendous enthusiasm around it. This is due to the mind-boggling speed, lower latency, and greater capacity compared to the previous generation of 4G wireless standards.

One of the best features of 5G technology is that it is incredibly agile and highly programmable. Its network slicing feature enables service providers to provide defined optimized resources to a specific user or area.

If we specifically talk about the broadcasting industry, 5G has great potential to transform the audience experience and bring new revenue streams for media transmitters. From live event streaming to the real-time immersive experience, along with innovative advertising set-ups, 5G can be instrumental in creating a whole set of a new gamechanging ecosystem. It gives broadcasters an edge to expand their capabilities to reach out to millions of mobile subscribers directly, making their content more accessible than ever.

The transition to 5G will empower media producers to stay mobile while creating, transmitting content, and capturing live-action without wired networks restraints. It will enable subscribers to stream higher quality Ultra-High-Definition (UHD) content seamlessly, refining their viewing experience. Through advanced analytics and algorithms, media companies will be better equipped to provide tailored audio and video feeds to their subscribers on their smart devices. The industry might witness concepts such as exclusive content broadcasting for their premium customers in the next few years.

However, to make 5G dreams a reality for India, it is critical accelerating nationwide fiberization and make aggressive network infrastructure investments so that even rural India can experience the next level of entertainment without any interruptions.

"The transition to 5G will empower media producers to stay mobile while creating, transmitting content, and capturing live-action without wired networks restraints."

डिजिट
अब हिंदी में

देश का सबसे लोकप्रिय और विश्वसनीय टेक्नोलॉजी वेबसाइट डिजिट अब हिंदी में उपलब्ध हैं। नयी हिंदी वेबसाइट आपको टेक्नोलॉजी से जुड़े हर छोटी बड़ी घटनाओ से अवगत रखेगी। साथ में नए हिंदी वेबसाइट पर आपको डिजिट टेस्ट लैब से विस्तृत गैजेट रिव्यु से लेकर टेक सुझाव मिलेंगे। डिजिट जल्द ही और भी अन्य भारतीय भाषाओ में उपलब्ध होगा।

digit.in
NOW IN HINDI

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

डिजिट

LAUNCHING

digit SQUAD

MEHENG 12896/13/1/2011-TC DATED18/05/2011

Here is your chance to become a Digit certified tech influencer

Benefits of Digit Squad Member

- Launch your own tech channel on Digit.in
- Become a Digit Certified tech influencer
- Engage with digit editorial team
- Make money

Apply now by scanning the QR code

www.digit.in/digit-squad/apply.html