Column
Spotlight: Low-Code/ No-Code Pg 06

Insight
Understanding The Digital Age: Cybersecurity, Privacy, And Data Protection Pg 33

Volume 12
Issue 09
November-December 2023
₹150

25th ANNIVERSARY CIO&LEADER

TRACK TECHNOLOGY • BUILD BUSINESS • SHAPE SELF

TECH HONCHOS SPOTLIGHT 8 TRENDS SHAPING ENTERPRISES IN 2024

AI transformation, cybersecurity strides, data integrity, and immersive experiences lead enterprise priorities.

A 99 Group Publication

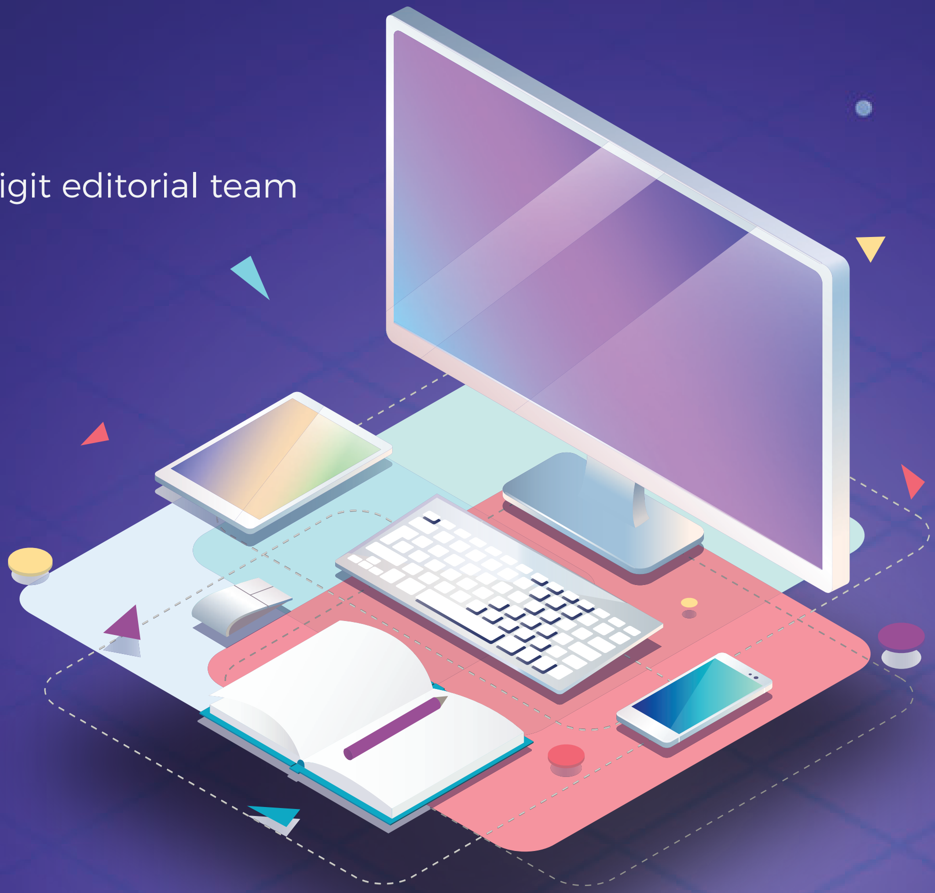
LAUNCHING

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

Shyamanuja Das
shyamanuja.das@9dot9.in

PPP 2.0

No one has seen tomorrow. That doesn't stop analysts and media from forecasting the future occasionally because they give something to work towards.

When it's near-term predictions, usually, practitioners have a better tap because no one knows better than them what they are up to. Yes, in the short term, they influence the future the most.

Various factors influence technology adoption. Some supply-side forces include technology development, the number of technology companies backing a particular technology, their market prowess, etc. The demand side forces have a competitive nature of a business segment, level, nature of regulation, technology maturity in a particular organization, and skill availability.

Of late, environmental factors have become important influencers of technology adoption by businesses. Most prominent among these is the growing consumerization of technology.

I would like to point out one such rising factor in India: the aggressive digitization of governance and citizen service infrastructure. While that itself is a catalyst of growing consumer digitization and is well-acknowledged, it can drive economic growth for the country and make businesses and the government more efficient by avoiding duplication in technology investment and even making them more effective by dramatically increasing reach. Call it Public Private Partnership (PPP) 2.0. It is something that will happen anyway. The idea is to accelerate it by becoming proactive.

India's DPI enhances sectors like health and education, offering mutual benefits for government and private companies in terms of revenue and efficiency.

Digital Public Infrastructure (DPI), which India has taken a lead in, can revolutionize its reach. The government has taken several initiatives in health, primary education, higher education, and civil supplies. Private companies can leverage them. The government will benefit from revenue and expertise. Businesses will gain in terms of reach and efficiency. ■

CONTENT NOVEMBER DECEMBER 2023

Cover Design by:
Vipin Rai

ADVERTISERS' INDEX

Sify	BC

This index is provided as an additional service.The publisher does not assume any liabilities for errors or omissions.

Please Recycle This Magazine And Remove Inserts Before Recycling

Printed and published by Vikas Gupta for Nine Dot Nine Mediaworx Pvt Ltd, 121, Patparganj, Mayur Vihar, Phase - I, Near Mandir Masjid, Delhi-110091. Printed at Tara Art Printers Pvt ltd. A-46-47, Sector-5, NOIDA (U.P.) 201301

CIO&LEADER

www.cioandleader.com

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

EDITORIAL
Group Editor - 9.9 Group: **R Giridhar**
Editorial Director - B2B Tech: **Shyamanuja Das**
Executive Editor - B2B Tech: **Jatinder Singh**
Principal Correspondent-B2B Tech: **Nisha Sharma**

DESIGN
Associate Art Director: **Baiju NV**
Sr. UI UX Designer: **Nikhil Wahal**
Sr. Designer: **Vipin Rai**

SALES & MARKETING
Executive Director - B2B Tech:
Sachin Nandkishor Mhashilkar (+91 99203 48755)
Associate Director - Enterprise Technology:
Vandana Chauhan (+91 99589 84581)
National Sales Head-B2B Tech:
Vaibhav Kumar (+91 97176 74460)
National Digital Head:
Kaizad Patel (+91 98208 20998)
Brand Manager:
Sheena Dawar
Senior Manager - Community Development:
Neelam Adhangale (+91 93214 39304)

Regional Sales Manager
North: **Pratika Barua (+91 9999510523)**
Ad Co-ordination/Scheduling: **Kishan Singh**

OPERATIONS
Head - Projects (Enterprise Technology): **Dipanjan Mitra**
Head - Digital & Event Operations: **Naveen Kumar**
Head - Digital Operations: **Atul Kumar Pandey**

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

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

SAP Embraces Gen AI Tools For Enhanced User Experience

SAP introduced SAP Build Code solutions, a pro-code companion to the low-code SAP Build environment, with extended GenAI capabilities.

By Jatinder Singh | jatinder.singh@9dot9.in

S**AP, a major ERP** software provider, is shifting from core ERP to integrating Gen AI tools, aiming to improve user-friendliness and optimize the user experience. The German enterprise software firm reiterated its commitment to embed GenAI capabilities in its product portfolio at SAP TechEd, an annual developers' conference.

During the conference, attended by numerous developers, SAP introduced SAP Build Code solutions, a pro-code companion to the low-code SAP Build environment, with extended GenAI capabilities. These tools streamline collaboration, specifically for SAP applications, allowing faster development of productivity tools. Optimized for Java and JavaScript, SAP Build Code utilizes SAP's generative AI copilot Joule to enhance productivity by embedding code generation capabilities for data models, application logic, and test script creation.

Developers creating applications or extensions for SAP solutions can now leverage Joule to generate code, develop data models, and test data. SAP Build Code's new generative AI capabilities make developing unit test scripts and testing applications for various scenarios easier.

With these new solutions, the company aims to empower developers and enhance SAP development productivity. The launch included three AI-infused products designed to streamline the SAP development process.

"The innovations we're launching at SAP TechEd, from AI-infused pro-code tools to a one-stop shop to create generative AI extensions and applications on the SAP Business Technology Platform, support the developers at the heart of the AI revolution and provide them with the resources they need to transform the way businesses run," said Juergen Mueller, Chief Technology Officer of SAP SE.

SAP's recent announcements underscore the growing importance of AI in the company's operations, with a commitment to upskill 2 million developers. Sindhu Gangadharan, Senior Vice President & Managing Director of SAP Labs India, highlighted the unprecedented opportunity in GenAI, noting its transformative impact in various sectors. ?The opportunity in GenAI is unprecedented and huge. In the last few months, we have seen an explosion of AI applications, particularly in healthcare, education, agriculture, and transportation, to name a few. The whole AI and large language models pioneered by OpenAI are truly transforming the way people interact with machines. As a technologist who has been around for over two decades, I have not seen anything as powerful before," she said.

GenAI is changing how businesses and users interact, particularly as the next generation adapts to rapid, digitally-enabled conversations, replacing traditional management approaches. McKinsey & Co. estimates that generative AI and related technologies could contribute up to $4.4 trillion to global GDP as automation becomes more prevalent between 2030 and 2060. SAP places significant emphasis on encouraging developers and partners to create AI solutions utilizing the capabilities offered by the Business Technology Platform (BTP).

Generative AI and related technologies could contribute up to $4.4 trillion to global GDP as automation becomes more prevalent between 2030 and 2060.

Emphasizing the integration of Generative AI into daily life and work, JG Chirapurath, Chief Marketing and Solutions Officer at SAP BTP and AI, highlighted the focus on responsible deployment, ensuring solutions generate responses based on real-world scenarios. ■

COLUMN

By Akash Jain

Spotlight: Low-Code/ No-Code

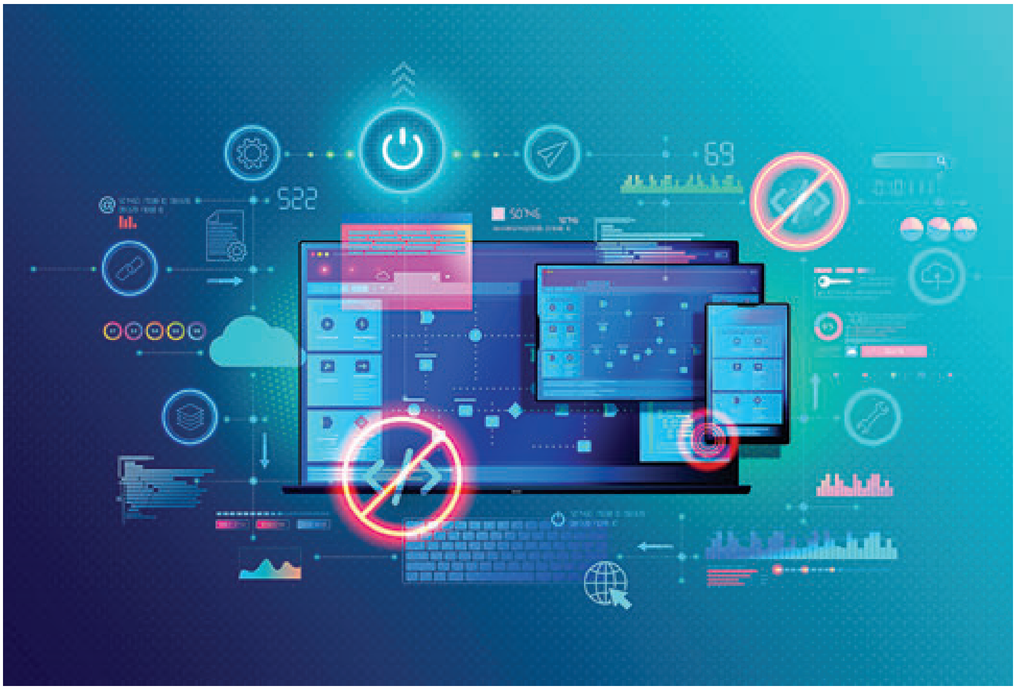
Low-Code/No-Code evolution traces from binary to Assembly, then high-level languages and functional programming, now vital in remote work and skill shortages era, balancing ease of use with IT compliance.

Before we delve into the current state, opportunities, and challenges of this column's topic, let us briefly examine how binary coding evolved into Low-Code/ No-Code. The zeroes and ones gave way to Assembly language, which was all about directly manipulating the binary. As silicon took over from vacuum tubes, programming languages were born. Hundreds emerged over the years, some highly specialized (e.g., concurrent, visual, etc.). Then came functional programming, which offered higher abstraction and bypassed lower-level details. Low-code and no-code were but a natural progression from functional programming. And this progression was accelerated by COVID-19, with remote work mandates and programming skills shortages. In fact, New York City (and soon after Washington D.C.) created a COVID-19 engagement portal to provide services, which was up and running in 3 days flat, with NO ONE writing any code.

Let us also differentiate between the two. Low-code requires a rudimentary level of programming acumen, while No-code is for citizen developers who need to gain programming knowledge. Low code has already penetrated many enterprises, consulting firms, and technology providers. It is now being predicted that No-code will eventually eclipse Low-Code. The reasoning behind this is straightforward and not worth spending time on.

As expected, Artificial Intelligence and Machine Learning are now increasingly used for Low-code/ No-code, which may soon stand on its head. And we may quickly see AI and ML developing applications independently. Essentially, software developing

The author, Akash Jain, 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.



software. A process called "program synthesis" is still considered to be in the 'ambition' stage. Koushik Sen, a professor of computer science at the University of California, Berkeley, calls No-Code an Amazon Alexa for programming. Just say what the input and output are, and get the coding done. Today, there are use-specific such/ similar applications; for example, Mendix is a platform that provides recommendations to developers as they are developing their Apps. The day of more generic and easy-for-all is not too far. Object-oriented programming has already created an army of citizen programmers ready and waiting.

Additionally, the rapid digitization of business and the need for macro-impact micro-decisions make Low-Code and No-code an increasingly attractive proposition for many enterprises. Remember that today's Low-code/ No-code platforms realize several benefits over previous generations of manually writing lengthy lines of code with low-level or high-level languages, especially the availability of used and proven algorithms. AND such micro-solutions can be combined to create complex solutions. Add to it the benefit of faster implementation of (more straightforward and specific) business solutions; this allows businesses to respond faster to today's dynamic environment.

The main problem is that no human may understand the code developed because it will have no comments, and the variable names will be inscrutable. And code efficiency will have the logic that will be difficult to comprehend.

However, McKinsey says Low-Code can turn 'Shadow IT' into a technology asset. This will be increasingly possible with No-code. Shadow IT is essentially the ecosystem of spreadsheets and documents that employees create for use by self or their teams and are (usually) used to make critical decisions. These may never get institutionalized, and IT Departments are often unaware of their existence. And therein lie the security and compliance risks. A huge risk with this operation is that Shadow IT, which often uses the 'official' IT data, can get disrupted as IT changes (potentially disrupting business operations).

If we look at the challenges, Security and Compliance come to mind (compounded manifold by no code). And, as low-code/no-code is entering the realm of AI, ML, and RPA, the security and compliance risks will get compounded. According to the MIT Sloan Management Review, the solution is creating an official platform for developing, propagating, securing, and regulating such applications.

Thus, increasingly, the role of the IT Department will include managing a platform for the erstwhile Shadow IT; even Microsoft Excel, with its (custom and shared macros, is all it might take). This will entail a higher degree of security and compliance monitoring because IT must know what is coming from where! In a mature environment, the IT Department will propagate a new low-code/ no-code business application within and/ or across business functions. Sometimes, they must "generalize" the application to make it worthwhile for other departments. Work will always be needed to integrate these applications into the core IT system and change these as the core IT Applications change.

In summary, Low-code/ No-code takes IT to where real operational business decisions are made ("edge computing" of business decisions!!). And this makes it a two-edged sword. An enterprise can end up in dust with the security or compliance breach(es) of an employee who is not rogue but not sufficiently trained on these. OR, the enterprise can benefit from the ease of decision-making using specific tools developed by the users who WILL use them. It is now up to the IT Department to choose its path: institutionalize "Shadow IT" or keep the fingers crossed while looking the other way. ■

TECH HONCHOS SPOTLIGHT 8 TRENDS SHAPING ENTERPRISES IN 2024

AI transformation, cybersecurity strides, data integrity, and immersive experiences lead enterprise priorities.

By **Nisha Sharma** | nisha.sharma@9dot9.in

The tech landscape experienced a seismic shift in 2023, marked by the rise of transformative technologies such as Generative AI, a growing emphasis on automation, and the delivery of exceptional digital experiences. As GenAI quickly moves from an emerging technology to a productivity essential tool, CIOs and enterprises find themselves navigating its diverse use cases and innovative applications amidst a cautious approach, addressing challenges posed by emerging threats and skillset gaps.

For CIOs, 2023 posed the formidable task of crafting a resilient technology roadmap amid economic uncertainties. GenAI, a hot topic among CIOs, is set to integrate seamlessly into business strategies in 2024, aligning with Gartner's predictions.

A significant milestone of the year was the enactment of the Digital Personal Data Protection (DPDP) Act by the Indian Parliament on August 11, 2023. This legislation reshapes India's data management framework, underscoring the pivotal role of Data Protection Officers (DPOs) in ensuring compliance and upholding data privacy. With plans to make the Digital Personal Data Protection Law live in 2024, technology leaders will remain at the forefront, deciphering the impact of these laws on the enterprise ecosystem and determining the necessary steps for preparedness. Simultaneously, the US government and the European Union are in the advanced stages of implementing robust laws to regulate AI, presenting several challenges and opportunities for the growth of technologies like AI.

Amidst these dynamic shifts, CIOs and CISOs find themselves at the crossroads of adapting to technological advancements. This edition delves into the top tech focus areas for enterprises in 2024, drawing insights from discussions with influential CIOs and industry leaders.

1. AI to Drive Intelligent Transformation

In 2024, integrating artificial intelligence (AI) and machine learning (ML) will fundamentally transform customer experiences and refine risk management across diverse industries. Beyond external customer interactions, such as AI-powered chatbots, these technologies are now pivotal for internal processes and risk assessments in various sectors.

Customer engagement and predictive analysis:

For many CIOs, The emphasis has shifted away from basic applications such as sentiment analysis to more complex tasks such as customizing investor communications and generating detailed analytical reports. This headway highlights the growing reliance on AI and ML for comprehensive customer profiling and predictive analysis, allowing businesses to effectively anticipate and mitigate potential risks.

According to Ananth Subramanian, EVP, and Head IT, Kotak Mahindra Asset Mgt, "While we had started consuming some of these (AI) services to do sentiment analysis, we are now exploring areas where we could customize responses to investors' emails. Other use cases have generated summarized reports after feeding multiple inputs on a specific stock. We have also started adopting platforms to improve our IT risk monitoring areas. These include correlation with system metrics to provide UEBA and and look at possible anomalies that can come up in the future."

Global impact of data-led businesses: Globally, data-led businesses are poised to disrupt the landscape with smart strategies harnessing data for purposeful gains. AI is reshaping organizational operations, customer interactions, and overall value creation. AI initiatives are driving differentiated strategies in customer engagements, business and strategic planning, research and development, financial operations, and supply chain management, spanning across industries.

Embarking on this AI journey, KRC Murthy, Senior President & Head IMG - Business & Digital Technology Solutions at Yes Bank, shares, "AI and machine learning have become integral components of our business strategy, standing the test of time as we extensively leverage them across our entire end-to-end customer journey. This utilization extends beyond external customers to encompass internal end-users, aligning with the prevailing trend. Our AI journey enables comprehensive 360-degree customer profiling, contributing significantly to our business trajectory."

Leveraging automation for cybersecurity:

While AI-powered security tools have been increasingly adopted for threat detection and response, the industry is also dealing with challenges such as growing false positives when new data doesn't match historical patterns, posing a challenge for these tools and solutions.

Looking ahead to 2024, advanced authentication methods such as AI biometrics are expected to add an extra layer of security to the enterprise ecosystem. The role of automation and orchestration is also likely to grow in streamlining incident response, reducing manual intervention and response times.

According to Harshad Mengle, CISO at Tata Chemicals Ltd, "AI and ML algorithms analyze vast datasets to identify patterns and anomalies, improving the ability to detect potential threats. Additionally, blockchain enhances data integrity, while automation and orchestration streamline incident response, reducing manual intervention and response times. Integrating advanced authentication methods, such as biometrics, also bolsters security measures. These technologies collectively fortify security systems against evolving threats."

AI's utilization in physical security, especially through video analytics and facial recognition in surveillance, is on the rise. The financial and healthcare sectors are exploring the deployment of AI-based tools for fraud detection and safeguarding patient data, respectively. In manufacturing, AI is anticipated to take a central role in surveillance and predictive maintenance, proactively mitigating risks on factory floors. The retail sector experiences the positive effects of AI in curbing shoplifting and fraud through smart cameras and transaction analysis, showcasing the widespread impact of AI on industry-wide security.

Satyavrat Mishra, Head - Corporate IT & Group CISO, Godrej Industries, said "So I think in 2024, our key focus is going to be, you know, data, AI, ML, and the use of

ANANTH SUBRAMANIAN
EVP, and Head IT,
Kotak Mahindra Asset Mgt

★ ★ ★ ★ ★

> **"While we had started consuming some of these (AI) services to do sentiment analysis, we are now exploring areas where we could customize responses to investors' emails."**

SURESH KUMAR

Partner and CIO, Grant Thornton

> “The prominent trend in 2023, expected to become increasingly prevalent, is GenAI. The persistent challenge of cybersecurity looms large as hackers adeptly leverage AI and GenAI to craft sophisticated phishing and hacking attacks. CIOs must remain vigilant, staying ahead by keeping their eyes and ears open to the evolving landscape.”

Gen AI to improve overall employee productivity. Data, as you know, has increased over time, and it is crucial to use this acquired data to run advanced algorithms, etc., to derive value. Therefore, must take it to the cloud and use some of the new edge pass solutions, either in Azure or AWS, and then build dashboards and provide insights to the business. Also, since AI and ML are going to play a very important role, especially in organizations like consumer products, etc., right? Because the data volumes are very large.”

Natural Language Processing (NLP): NLP advances enhance AI's language understanding. In 2024, expect sophisticated models, emotional AI, and multimodal interactions to revolutionize conversational AI. Real-time translation and contextual understanding intensify. Kapil Mehta, Sr. Director, Technology Solutions of Visionet, highlights immersive experiences through diverse communication modes, emphasizing the importance of real-time language translation in conversational AI. Improved contextual understanding enables chatbots to maintain longer conversations, offering personalized responses based on historical interactions.

Across organizations, varying adoption stages of AI and ML reflect a universal acknowledgment of their indispensable role in the future success of business intelligence.

2. Democratization of Gen AI: Transformative Shifts and Cautious Optimism

Generative AI, driven by revolutionary tools like ChatGPT, has swiftly moved beyond mere buzzword status, marking a business imperative within just over a year since its launch. A 2023 study from the University of Pennsylvania reveals a potential impact on approximately 80% of the US workforce, with at least 10% of their tasks influenced by large language models (LLMs), foundational to machine learning (ML) algorithms for generative AI.

From experimentation to strategic integration: The year 2023 represents a key turning point in the evolution of GenAI, transitioning

KRC MURTHY

Senior President & Head IMG – Business & Digital Technology Solutions at Yes Bank

> “AI and machine learning have become integral components of our business strategy, standing the test of time as we extensively leverage them across our entire end-to-end customer journey.”

from experimental phases to more strategic and impactful applications. As Generative AI becomes increasingly woven into core business strategies and daily workflows, the shift from technical fascination to intentional and strategic integration signals the onset of a new era—' intentional AI'—addressing real-world demands and fostering substantial business growth.

Deepak Bhosale, AVP-IT at Asian Paints, emphasizes the differentiating role of Generative AI, exerting a disruptive influence across personal and corporate lives. Revolutionary technologies like ChatGPT are setting new trends in enterprises, catering to massive customer demand and creating human-like capabilities.

CIOs anticipate a strategic application of AI and automation by a broader range of organizations, specifically in back-office and shared-service functions, with the aim of enhancing productivity and efficiency. According to Suresh Kumar, Partner and CIO, Grant Thornton, "the prominent trend in 2023, expected to become increasingly prevalent, is GenAI. The persistent challenge of cybersecurity looms large as hackers adeptly leverage AI and GenAI to craft sophisticated phishing and hacking attacks. CIOs must remain vigilant, staying ahead by keeping their eyes and ears open to the evolving landscape."

Overall, organizations, regardless of size, will persist in exploring how generative AI can provide a competitive edge, enhance customer value, and drive success. Amit Luthra, Managing Director, India, Lenovo ISG, underscores the pivotal role of Large Language Models (LLMs) in powering Gen AI, transforming natural language understanding, and revolutionizing customer interactions.

Global impact and economic potential: A prevailing consensus within the industry is that GenAI will fundamentally reshape the organizational structure and operations of businesses. In 2024, tech honchos expect a defining year where GenAI will undergo further democratization. Organizations will witness the rapid emergence of real-use cases, accelerating the pace at which their teams can redirect efforts toward higher-value work that aligns seamlessly with future business essentials.

On a global scale, McKinsey reports that Generative AI could potentially contribute between $2.6 trillion and $4.4 trillion annually across 63 specific use cases, amplifying the overall impact of AI by 15-40 percent. These estimates could double with the seamless integration of generative AI into existing software.

Pushkar Rege anticipates that the IT function will eventually transition into an AI function, showcasing the rise of Gen AI. Dhananjay Ganjoo, Managing Director for India and SAARC at F5, looks into the future, foreseeing the increased role of AI in enhancing real-time decision-making, addressing security concerns, and improving search engine outcomes. The strategic integration of AI into API testing is poised for widespread adoption in 2024, ensuring robust performance. These collective perspectives highlight the transformative impact of Gen AI across diverse sectors and the cautious optimism surrounding its future applications.

According to Deloitte's Tech Trends 2024 report, the foreseeable future may usher in a scenario where businesses find it increasingly seamless to reap the rewards of GenAI within their industries. This anticipation is driven by the emergence of models trained on more specific data, marking a departure from the current trend where AI models are constructed upon foundational models that were trained on general-purpose data.

PUSHKAR REGE
CIO at UPL

★ ★ ★ ★ ★

> “We are dedicated to focusing on smart manufacturing and privatizing it. It's a marathon, and we are already partway through the journey.”

DEEPAK BHOSALE
AVP-IT at Asian Paints

“Revolutionary technologies like ChatGPT are setting new trends in enterprises, catering to massive customer demand and creating human-like capabilities.”

3. Focus on Data Integrity, Trust, and Advancing Cybersecurity Skillsets

As businesses expand their digital operations, CIOs are increasingly prioritizing data integrity, fostering trust, and enhancing their teams' cybersecurity skills. In 2023, organizations embraced advanced security practices such as vulnerability assessments, penetration testing, and the implementation of multi-factor authentication. This reflects a proactive approach to mitigating digital threats.

Impact due to new AI models: According to Gartner, the democratization of access to AI has made the need for AI Trust, Risk, and Security Management (TRiSM) even more urgent and clear. Without guardrails, AI models can rapidly generate compounding negative effects that spin out of control, overshadowing any positive performance and societal gains that AI enables. Gartner predicts that by 2026, enterprises that apply AI TRiSM controls will increase the accuracy of their decision-making by eliminating up to 80% of faulty and illegitimate information. AI tools have provided cybercriminals with a strategic advantage, enabling them to deceive their targets by impersonating others. This makes it exceedingly challenging for users to discern and identify potential threats.

Cybersecurity and Digital Technology Expert Kanishk Gaur notes that, in the face of increasingly sophisticated digital threats, the focus will be on implementing multi-layered security strategies. This includes advanced threat detection systems, regular cybersecurity audits, and employee training programs to ensure vigilance and preparedness against potential cyber threats.

In 2024, the industry expects widespread adoption of the zero-trust security model, underscoring a commitment to continuously evolving security strategies. This trend indicates a shift from traditional, perimeter-based security to a more dynamic, holistic approach.

Mandy Andress, CISO, Elastic, commented on this, saying, “In 2023, cybersecurity continued to face a mix

SATYAVRAT MISHRA
Head - Corporate IT & Group CISO, Godrej Industries

“In 2024, our key focus is going to be, you know, data, AI, ML, and the use of Gen AI to improve overall employee productivity.”

of continuity and change, with social engineering persisting and the cloud reshaping the landscape. In tandem, AI is evolving, and responsibility for incidents has also shifted to treat companies more as victims."

Regular audits and employee training: CIOs highlight the need for continuous improvement in cybersecurity skill sets. This proactive approach ensures a robust defense against the dynamic landscape of cyber threats and evolving IT governance guidelines. The evolution in cybersecurity practices signifies a pivotal adaptation to safeguard data integrity and uphold trust in the digital era.

The integration of these comprehensive security measures is crucial for maintaining.

Integrating these comprehensive security measures is essential in maintaining the trust and integrity that are cornerstones of the banking and financial industry, underscoring a broader movement towards more sophisticated, integrated, and proactive cybersecurity measures across industries, recognizing security's paramount importance in the digital transformation age.

Real-Time AI-driven Security Operations Centers (SOCs): As organizations grapple with the imperative to fortify their cybersecurity defenses, the integration of AI and automation emerges as a pivotal strategy, promising to elevate the efficacy of SOC teams. In the year 2024, the industry will see the rise of AI and automation within the SOC team as manual detection and response processes are proving inadequate.

Against this backdrop, Manish Grover, Executive Director, Strategic Information Systems, IOCL, sheds light on the evolving cybersecurity landscape, particularly in the energy sector. He notes,"There's a growing emphasis on enhancing cybersecurity measures in the energy sector. Companies are increasingly adopting sophisticated security practices, including establishing around-the-clock (SOCs) and adhering to international standards like ISO 27001. This approach encompasses comprehensive vulnerability assessments and penetration testing across various infrastructures and applications. Deploying multi-factor authentication, anti-APT tools, advanced endpoint security, and gateway security tools reflects a proactive stance in safeguarding sensitive data. Furthermore, the shift towards a Zero Trust security model demonstrates a commitment to continuously evolving cybersecurity strategies to address emerging threats," says Manish Grover.

Elia Zaitsev, CTO of CrowdStrike, emphasizes, "To stop modern adversaries in 2024, the SIEM needs to be rebuilt from the ground up for the SOC around the security analyst experience. The market will dictate a need for solutions that unify all capabilities, including SIEM, SOAR, EDR, and XDR, into one cloud-native, AI-powered platform to deliver better, faster, and more cost-effective outcomes."

MANISH GROVER

Executive Director, IOCL

> **There's a growing emphasis on enhancing cybersecurity measures in the energy sector. Companies are increasingly adopting sophisticated security practices, including establishing around-the-clock SOCs and adhering to international standards like ISO 27001.**

4. Network and Infra Modernization for Future Readiness

n 2024, CIOs and technology leaders will continue to prioritize network modernization. As enterprise operations increasingly revolve around cutting-edge technologies such as AI, and the demand for faster connectivity intensifies, relying on outdated networks becomes impractical. The crucial task is to align with networks that not only keep pace with these advancements but also can accommodate the necessary computing power.

Extending the focus from ERP to SaaS upgrades, the emphasis lies on implementing top-notch cloud solutions capable of supporting modern engineering. CIOs will persist in steering their networking and IT infrastructures toward the cloud, enhancing capabilities for

SUSHIL MEHER

Head-Health IT, AIIMS

> **“Things are changing very fast. We need new people who can adopt new technologies in advance so that they can have their state. They can play a major role and give new opportunities to new people and the old generation.”**

seamless navigation across public clouds, data centers, and edge infrastructures cost-effectively.

As Deloitte predicts in its recent report on 2024 Tech trends, many companies have experienced subpar transformation programs that amounted to massive bets on a single dimension of their core systems, which ultimately failed to deliver the benefits promises. Instead of undertaking random acts of innovation or "low-hanging" transformation investments, technology leaders may need to face a hard truth: Their technology house is ailing. And they need new ideas for where to focus time and effort so they can begin to heal.

5. Blockchain's Surge for Operational Efficiency and Enhanced Security

The blockchain technology market at the global level is developing at a rapid rate, and in the upcoming few years, it is expected to grow significantly.

In 2015, Transparency Market Research revealed that the global market for blockchain technology was worth US$315.9 mn, and the value will surpass US$20 bn by the end of 2024.

While many existing studies have highlighted the implications of blockchain technology on business operations to achieve productivity, sustainability, and resilience, it is pivotal to comprehensively examine which business operations, functions, activities, and sectors will reap the most benefits.

Manish Grover, Executive Director, Strategic Information Systems at IOCL, shared that Indian Oil is currently in the early stages of adopting blockchain technology with a strong commitment to enhancing its operational efficiency and customer service. Their strategic focus areas for exploring blockchain applications include supply chain management, payment security, trade finance streamlining, data protection, and the implementation of smart contracts.

Analytically, these initiatives enable real-time data visibility and insights, reduce fraud risk, optimize time and cost-related key

HARSHAD MENGLE

CISO at Tata Chemicals Ltd.

> **“While 5G offers faster speeds and lower latency, it introduces new security considerations, requiring robust encryption for data in transit.”**

performance indicators, enhance data security, and automate processes, all of which contribute to data-driven decision-making and operational improvements.

6. Enhancing User Engagement through Immersive Experience

Anticipated in 2024 is a significant surge in focusing extensively on enhancing user engagement through immersive experiences. While virtual reality (VR) and augmented reality (AR) are not new concepts, they have transcended their gaming origins to become transformative tools across various industries.

In the retail sector, there is a noteworthy emphasis on leveraging AR and VR technologies for virtual try-ons and product demonstrations, providing an innovative and interactive shopping experience.

From manufacturing to customer interactions, these technologies are revolutionizing how businesses engage with products, services, and the digital realm. A domain witnessing a profound impact is product lifecycle management (PLM).

In manufacturing, the adoption of AR and VR technologies is gaining momentum to strengthen employee training and operational efficiency. These technologies are not only being evaluated for internal purposes but also to assist end customers, like plumbers, in training scenarios. AR and VR facilitate intricate training simulations, reducing material waste and fostering sustainability.

This strategic incorporation of AR and VR in manufacturing reflects a notable shift toward utilizing technology to enhance training effectiveness and optimize resource utilization, showcasing a commitment to innovation and sustainable practices in the industry.

7. Efficiency Enhancement in Business Operations

In 2023, technology leaders were confronted with the challenge of achieving more with fewer resources, a sentiment frequently shared during interactions with CIO&Leader. Organizations felt a growing pressure to optimize their business processes, utilizing various cloud technologies to simultaneously cut costs and foster innovation. In the manufacturing sector, the spotlight has been on smart manufacturing as a key area of focus.

Looking ahead to 2024, an apparent shift toward a pragmatic approach is anticipated in the manufacturing sector. The enthusiastic proclamations about generative AI, the industrial metaverse, reshoring manufacturing jobs, and autonomous vehicles are expected to be tempered by the sobering realities of addressing issues such as technical debt, legislation, and navigating global supply chains.

Pushkar Rege, CIO at UPL, encapsulates this approach, stating, "Smart Manufacturing is crucial for a core manufacturer like us, serving over 55 countries. We are dedicated to focusing on smart manufacturing and privatizing it. It's a marathon, and we are already partway through the journey. We aspire to be swift followers in this context, leveraging our existing presence in the cloud. While there is considerable hype about the cloud and cost, we view it as a journey we are enthusiastic about and confident in." This perspective underscores the commitment to a thoughtful and strategic evolution, acknowledging the complexities of the business landscape while embracing the transformative potential of technology.

8. Significant Uptake of Enterprise 5G

With more and more workloads moving to the cloud, enterprises prioritize secure network modernization, driving interest in 'Captive Non-Public 5G Networks.'

KANISHK GAUR
Cybersecurity and Digital Technology Expert

★ ★ ★ ★ ★

“In the year ahead, the focus will be on implementing multi-layered security strategies. This includes advanced threat detection systems, regular cybersecurity audits, and employee training programs to ensure vigilance and preparedness against potential cyber threats.”

FOCUS AREAS FOR ENTERPRISES IN 2024

GenAI Impact:
Expected to boost creative problem-solving time by up to 50%, GenAI will drive customer-centric innovation, creating substantial business value.

AI Strategies:
AI continues as a crucial force for enhancing customer experience and promoting innovation. Enterprises invest in AI tools like synthetic data and TuringBots for faster, cost-effective software development.

Modern Infrastructure Investment:
Decision-makers plan investments in network, end-user hardware, and data center infrastructure.

SaaS Adoption:
A shift towards SaaS is imminent, with only 25% of enterprises expected to retain on-premises software by 2024.

Optimizing Cloud Environments:
Amid increasing cloud investment, leaders will assess new environments for broader IT design and seamless workload shifts.

Autonomous Workplace Assistants:
GenAI's progress will drive experimentation with AWAs, aiming to accelerate workplace productivity and innovation.

Tech Talent Management:
With certain tech skills, especially in AI, remaining scarce, technology leaders will focus on strategic collaborations with industry and stakeholders.

Customer Experience (CX) Improvement:
CX is expected to improve for the first time in years, thanks in part to GenAI helping customer service agents answer questions faster and better.

Source: Forrester's Predictions and Insights for 2024, Forrester's 2024 Planning Guides

The CIOs expect a surge in enterprise 5G trials and projects in 2024.

Harshad Mengle underscores the challenges, noting that while 5G offers faster speeds and lower latency, it introduces new security considerations, requiring robust encryption for data in transit.

Enterprise 5G, with its lowered latency and assured reliability, becomes instrumental in advancing augmented reality, virtual reality, and IoT applications across diverse sectors like healthcare, education, manufacturing, and smart cities. It serves as a crucial infrastructure for various AI workloads.

The distinctive advantage of enterprise 5G lies in its cloud-native technology, specifically its standalone (SA) mode, supported by features like network slicing, end-to-end orchestration, and automation. Amit Luthra, Managing Director, India, Lenovo ISG, highlights the pivotal role of the fusion of 5G and Edge Computing, overcoming challenges through real-time data processing.

5G will bring a significant shift in Security Operations

Significant emphasis will be placed on integrating edge computing into enterprise network modernization initiatives, aiming to mitigate latency and elevate overall performance. The dynamic collaboration between 5G and edge computing is poised to unlock novel possibilities across various industries. Sectors such as manufacturing, logistics, and healthcare stand to harness this powerful combination for real-time monitoring, predictive maintenance, and personalized services.

Harshad Mengle underscores the operational intricacies of edge computing, emphasizing the need for a distributed and scalable infrastructure. Effectively managing a network of edge nodes necessitates the adaptation of data center management practices. This involves the implementation of robust security measures, ensuring high availability, and adeptly managing diverse hardware at different locations. In essence, the widespread adoption of edge computing is reshaping the strategic positioning and management of data centers to align with the evolving demands of distributed computing.

In addition, in 2024, CIOs will be directing their attention to critical areas such as spearheading sustainability and ESG initiatives, optimizing data center costs, and maximizing the value derived from their data centers. ■

Robust Security Platforms Crucial For AI Risk Mitigation

By **Jatinder Singh** | jatinder.singh@9dot9.in

GEOFF SWAINE
Vice President, APJ, CrowdStrike

Geoff Swaine, Vice President, APJ, CrowdStrike emphasizes on the critical balance between speed and visibility in the exclusive conversation with CIO&Leader.

As IT infrastructures become more complex and distributed, enterprises face the formidable task of safeguarding users, data, applications, systems, and networks from relentless attacks. Compounding this complexity is the pervasive adoption of Generative AI (GenAI) and the onset of the Automation era. In response, organizations find themselves compelled to refine and rationalize their cybersecurity strategies, seamlessly blending technological advancements with human intervention.

In a recent interaction with CIO&Leader **Geoff Swaine, Vice President, APJ, CrowdStrike** delves into this dynamic cybersecurity landscape. Swaine emphasizes the critical balance between speed and visibility. The conversation explores the intricate interplay of technology and human insights in adapting to changing cybersecurity trends, shedding light on the profound impact of GenAI and the ongoing shift in the automation era. Excerpts.

CIO&Leader: What are the key trends in the cybersecurity landscape, and how do these reflect the evolving threat landscape?

Geoff Swaine: The common thread revolves around speed. You may have seen a global threat report that we release every year, and every year, we observe the time it takes for a threat actor to move laterally from one system to another decreasing. It used to be that only nation-state threat actors had access to high-speed attacks. We are now seeing this trend in organized crime and other parts of the threat landscape. Speed is critical for security, but visibility is equally important. You must be able to see everything, and observability is a crucial part of the issue we have been observing, as observability is getting harder and harder.

Real-time quality monitoring and observability pose significant challenges for businesses across sectors, especially considering the evolving nature of threats. Organizations are increasingly focusing on these aspects due to the dual concerns of enhancing security and reducing costs. There are more and more data sources, making it increasingly challenging to build queries to identify events. CrowdStrike has been exploring this space for some time, making investments a couple of years ago in our approach to observability. We need to converge these two platforms closely together.

CIO&Leader: Given the growing adoption of AI in all facets of enterprise development, what primary security considerations should enterprises and CIOs prioritize?

Geoff Swaine: In DevOps and cloud operations, seamless interaction with processes and information is paramount. However, integrating AI introduces challenges, particularly in addressing perceived security threats.

One primary concern revolves around the actions of large language models. Understanding the operations of these models, the assets they leverage, and ensuring privacy around the data they utilize are vital considerations. Maintenance of AI models is another focus point — questioning whether there is any unauthorized access to train the models in undesirable ways, potentially leading to what is colloquially known as "AI hallucination."

Moreover, copyright, digital rights management, and governance issues become pronounced when AI generates content. For instance, the reliability of AI-generated business documentation or process flows comes under scrutiny, with potential security concerns arising from indirect prompt injections, where models may be trained to execute commands that pose harm.

From the perspective of CrowdStrike, a company deeply embedded in AI, the emphasis is on viewing AI as more than just an interface for large language models. The commitment is to leverage AI to discover the unknown and enable flexible workflows beyond the constraints of traditional sequential processes. The advice is to exercise caution, acknowledge the intricate nature of AI development, and ensure that security platforms are consistently updated to monitor and control potential risks.

Despite the challenges, the narrative acknowledges the excitement surrounding AI's transformative potential, especially in a resource-constrained economy. Harnessing AI efficiently becomes paramount for creating numerous job opportunities, particularly at the entry level, and optimizing automation to address various societal and economic needs. As organizations venture into this exciting territory, a balanced approach, blending enthusiasm with caution, is essential to unlock the full potential of AI in enterprise development.

CIO & Leader: Can you delve into the security challenges of GenAI and how organizations can navigate them?

Geoff Swaine: The emergence of generative AI introduces new opportunities for interaction with this critical data, requiring heightened caution. It is essential to recognize that generative AI, while enhancing productivity, requires careful consideration of ownership and management of the outcomes.

Organizations must be vigilant internally with their teams using generative AI and externally when interacting with others' IP. The potential for AI to build itself into a hallucination, following logical loops that may result in incorrect answers, underscores the importance of human oversight and appropriate validation. Security designers have witnessed instances where aggressive training models on AI can lead to inaccuracies, reinforcing the need for meticulous checking and human involvement.

Verification is anticipated to play a crucial role in the evolving landscape, offering a mechanism to ensure clarity and correctness in AI outputs. This, however, does not diminish the constant need for security. As AI generates and evolves, it introduces additional layers of data that require careful handling. The evolving nature of AI thinking, illustrated by the analogy of asking ChatGPT for a bread recipe evolving into sophisticated culinary instructions, underscores the importance of keeping track of each data generation.

This reality circles back to the initial emphasis on visibility and observability, where integrated platforms and tools in IT Ops contribute significantly. While these tools aid in managing the complexities, enterprise leaders face a significant challenge in securely comprehending the vast amount of data. Integrating observability, visibility, and data security remains a cornerstone in navigating the intricate landscape shaped by generative AI.

The conversation explores the intricate interplay of technology and human insights in adapting to changing cybersecurity trends, shedding light on the profound impact of GenAI and the ongoing shift in the automation era.

CIO&Leader: What specific innovations or strategies are being pursued to integrate security components seamlessly, thereby enhancing the capabilities of enterprises and businesses in this context?

Geoff Swaine: Addressing the challenges associated with the overwhelming volume of data, conventional SIEM technologies and log management tools often need to be revised due to the complexity of managing diverse sources and volumes. Extended query times have become a serious barrier, with queries taking exceptionally long durations, leading to significant inefficiencies. Some organizations have reported scenarios where queries initiated on Friday evenings would only yield results by Monday morning due to the intricate scripting required to navigate through the data complexity.

Another hurdle lies in data silos, where disparate data sources are spread across different locations, necessitating skilled resources to identify paths and streamline information flow. Given the scarcity of such professional resources and the potential costs associated with prolonged query times, a more efficient approach is imperative.

In summary, the ongoing pursuit of innovative strategies, compression techniques, and collaborative platforms underscores the industry's commitment to overcoming data-related challenges and optimizing efficiency in the post-health crisis landscape.

CIO&Leader: Can you elaborate on how the recent acquisition of Bionic enhances your cloud security capabilities, particularly in the evolving landscape where more organizations are adopting a cloud-native approach?

Geoff Swaine: The recent acquisition of Bionic is a testament to our commitment to advancing cloud

Organizations are cautious about investing in extensive and expensive security measures considering the economic landscape.

security. Our strength in runtime cloud security, encompassing aspects like API security, Cloud Identity and Entitlement Management (CIE M), and cloud workload protection, was already robust. With the addition of code-to-runtime protection capabilities, we've significantly elevated our cloud platform's capabilities. This enhancement allows us to understand how an application will run in the cloud and empowers the development team with valuable insights.

The convergence of DevOps practices, bridging the gap between development and operations within the cloud, is a crucial aspect of this advancement. This integration is poised to accelerate development cycles, marking a potential game-changer. As more organizations embrace a cloud-native approach, like ours, the experience we've gained in building large-scale, cloud-based, scalable architectures becomes invaluable. Managing vulnerabilities in such architectures is a complex task, and the synergy between Bionic and our existing robust security controls creates a compelling offering for our customers.

CIO&Leader: What cybersecurity trends are anticipated to define 2024, and what specific areas are you focusing on to address these trends?

Geoff Swaine: In the evolving landscape of cybersecurity, endpoint detection and response (EDR) and next-generation antivirus dynamics are undergoing a significant shift. The traditional antivirus solutions are gradually making way for the next generation, particularly EDR. Concurrently, we are witnessing continuous advancements in sandboxing, firewall technologies, and the emerging concept of secure access service edge (SASE), causing many changes in the cybersecurity domain.

The notable transformation we are currently observing is the ascendancy of the platform. CrowdStrike, in its strategic vision, has consistently advocated for a centralized platform featuring a unified user interface, a single agent, and a streamlined console. This simplicity spans security and cloud operations, fostering ease of use and efficiency. The uniformity in UI and console, irrespective of the operational domain, contributes to reducing the overall cost of monitoring and managing the platform.

In addition, the compliance environment, subject to constant reviews and revisions, is becoming more rigorous globally. Notably, recent regulation changes, such as those in Australia and Singapore, underscore the need for stringent compliance measures. This becomes particularly crucial in the Indian context, where the Data Protection and Privacy Act enactments signify a heightened emphasis on data protection. Maintaining compliance is not just a regulatory necessity; it's critical to securing and safeguarding data in the current regulatory landscape.

Organizations are cautious about investing in extensive and expensive security measures considering the economic landscape. However, the integrated approach of the platform is fast becoming a strategic choice for organizations striving for a balance between robust security and financial prudence.

As we navigate the current reality and anticipate positive shifts in the economy, the role of security remains non-negotiable. While investment opportunities emerge, security stands as a constant imperative. ■

DPDP Bill Is A Stride Towards A More Progressive And Secure Digital Future

DPDP bill can be seen as a significant step towards fostering an ecosystem of both protection and innovation.

By **Nisha Sharma** | nisha.sharma@9dot9.in

In the ever-evolving landscape of cybersecurity and digital consultancy, aspiring industry leaders must stay ahead of the curve, in an exclusive conversation with **Nisha Sharma** from CIO&Leader, **Akhilesh Tuteja,** the Global Head of Cyber Security Consulting and India Head of Digital Consulting at KPMG. He shared valuable insights and advice for emerging business leaders in this dynamic field.

Cultivating the right mindset

Tuteja underscores the importance of a growth mindset for leaders navigating the technological landscape. He believes that while technology plays a key role, a proactive and expansive perspective can enhance its benefits. Beyond just relying on current tech tools, Tuteja encourages leaders to move past traditional viewpoints. By doing so, they can better harness the full potential of technology, optimizing operations and opening doors to new opportunities.

Embracing diversity

Tuteja advocates for greater diversity in team compositions, highlighting its tangible benefits. Collaborating with individuals from a wide range of backgrounds and expertise not only brings varied approaches to problem-solving but also enriches the ideation process. Such diversity acts as a counter to the pitfalls of echo chambers, where similar thinking might stagnate innovation. By actively seeking and integrating diverse perspectives, organizations can ensure they are consistently at the forefront of innovation and best positioned for long-term success in a competitive landscape.

Willingness to experiment

In the rapidly changing landscape of cybersecurity, experimentation is critical. Tuteja emphasizes the importance of being open to trying new approaches, even if they don't always yield the desired results. This experimental mindset allows for continuous learning and adaptation, vital traits in an ever-evolving industry.

The future of cybersecurity

Looking ahead, Tuteja envisions cybersecurity not merely as a risk mitigator but as a trust enabler. As everything becomes increasingly interconnected, the role of cybersecurity transforms into an enabler for businesses to establish trust with their customers. He urges businesses to embrace cybersecurity to enhance customer experience and instill confidence in their products and services.

Adopting the Digital Personal Data Protection Bill

Tuteja applauds the Indian government's proactive approach to modernizing data protection regulations with the approval of the Digital Personal Data Protection Bill. He sees this as a significant step towards fostering an ecosystem of both protection and innovation. The bill simplifies compliance and enables businesses to view data through a business lens, unlocking new possibilities while minimizing risks.

> **Beyond just relying on current tech tools, IT leaders should move past traditional viewpoints to access technology potential.**

Conclusion

Akhilesh Tuteja's insightful advice and perspectives shed light on the critical aspects of cybersecurity and digital consultancy. Cultivating the right mindset, embracing diversity, and fostering a culture of experimentation are the cornerstones of success in the realm of cybersecurity. As technology continues to advance and intertwine with our lives, the importance of cybersecurity as a trust enabler cannot be overstated. The Digital Personal Data Protection Bill strives towards a more progressive and secure digital future, promising a delicate balance between innovation and safeguarding citizen interests. CIOs and industry leaders would heed these insights as they steer their organizations through tomorrow's exciting yet challenging cybersecurity landscape. ■

Generative AI And LLMs Are The Future Of Automated Responses

Gen AI
Generative AI will have a significant impact ac
sectors.
Generative artificial intelligence (AI) is artific
capable of generating text, images, or other m
to prompts or user inputs.
Generative AI models learn the patterns and s
input training data by applying neural Deep Le
generate new data that has similar pr
INDIA's FUTURE CIOs
NEXT 100
5TH CIO&LEADER SAMMAN
CIO&LEADER
Hartke
5TH CIO&LEADER SAMMAN
INDIA's FUTURE CIOs

The technolgical advancement leads to the lesser dependency on manual textual responses , and more on automation and efficiency.

By **Nisha Sharma** | nisha.sharma@9dot9.in

In today's digital age, automation has taken center stage. With the advancements in Generative AI and Large Language Models (LLMs), we're at the cusp of a revolution in automation, especially in sectors requiring textual responses. In our last 24th Annual CIO&Leader Conference, **Pradeepta Mishra,** Co-Founder and Chief Architect of Data Safeguard Inc. delved deeper into this fascinating world of automated text generation and saw how businesses can benefit.

The landscape of automated responses

From applications to product reviews, the need for automated responses is evident. One particularly pressing area is customer complaints. Pradeepta said, "Imagine a scenario: A business receives various complaints monthly. These complaints are typically categorized by service, price, or personnel issues."

Historically, businesses have maintained standard responses to each of these categories. With the emergence of LLMs, businesses can now automate this process.

Training an LLM begins with a pre-trained model. You then embed your data-questions or complaints in this scenario into this model. After fine-tuning, the model can provide a standard response when a related customer complaint occurs. This not only reduces manual intervention but also ensures a quick and consistent response.

Text-generation and summarization- a revolution

The application of LLMs isn't limited to customer complaints. LLMs have many use cases, from answering frequently asked questions (FAQs) without redirecting users to a URL to summarizing extensive legal contracts or terms and conditions.

"Think about the tedious task of reading a 20-page terms and conditions document. An LLM could potentially summarize this into actionable points, guiding a user on whether to proceed or reconsider."– Pradeepta added.

Moreover, these models can play a key role in generating social media content, automatically creating meeting minutes, and even scripting code. For example, for standard coding tasks, why reinvent the wheel when an LLM can generate the required code based on millions of similar examples.

The market players and architectures

OpenAI, a pioneer in the field, began its journey with data primarily from Wikipedia, however, the quality of data matters. The context is vital. If you train a model predominantly with novels and then ask business-related questions, it's bound to falter. Over the years, OpenAI has refined its models, with its latest being notably faster and more accurate.

As technology become more powerful and architectures more refined, enterprises will see a surge in industry leveraging Gen AI and LLM tools.

Speaking of architecture, there are primarily three-

- **Zero-shot architecture** involves a user giving prompts to a pre-trained model. It's free but offers lower accuracy.
- **Few-shot mode** merges a pre-trained model with some user-specific data for better accuracy. However, it needs more user data to handle.
- **Retrieval mode** is the most powerful and accurate but is also the costliest. It involves indexing the user prompts and data corpus for quicker and more precise responses.

Challenges ahead

As with any technology, there are concerns. For LLMs, the inclusiveness of training data is vital. The model's context understanding will only be as good as its fed data. Then, there's the paramount concern of data privacy and security, especially with personal or financial data. Furthermore, models have traditionally been limited in how much input text they can handle, although this is rapidly evolving.

Conclusion

The future is clear. Generative AI and LLMs will become integral to businesses. As models become more powerful and architectures more refined, we will see a surge in companies leveraging these tools. The blend of pre-trained foundational models with specific business data will become the norm. As technology advances, our dependency on manual textual responses will diminish, heralding a new era of automation and efficiency. ■

Embracing Innovation In Cybersecurity: A 2023 Outlook On Combatting Digital Threats

The rise of sophisticated cyber-attacks and the evolving nature of threats necessitate a dynamic and forward-thinking approach.

By **Nisha Sharma** | nisha.sharma@9dot9.in

As we commemorate International Computer Security Day 2023, the digital world is at a critical juncture, faced with unprecedented cyber threats. This year's observance brings into sharp focus the importance of embracing innovation and strategic foresight in cybersecurity. Insights from industry leaders like Geoff Swaine, VP of APJ at CrowdStrike, Karthikeyan G. Senior Director, Platform Engineering, at Ascendion, and Nilesh Kulkarni, Director of Qlik India, provide a comprehensive perspective on navigating this complex landscape.

The rising tide of cyber threats

Geoff Swaine, VP of APJ at CrowdStrike, paints a concerning picture of the current cybersecurity landscape. His observations, backed by the CrowdStrike 2023 Threat Hunting Report, reveal a 40% increase in interactive intrusions, with a majority being malware-free. This trend highlights the ineffectiveness of traditional cybersecurity defenses and the need for more adaptive and proactive solutions. Swaine's emphasis on the speed of adversaries, with breakout times reduced to 79 minutes, underscores the situation's urgency.

The advent of adversarial AI

Swaine also warns of the emerging threat posed by adversarial AI. The ability of generative AI to facilitate sophisticated social engineering attacks, especially in multiple languages, poses a new challenge in threat identification. This advancement lowers the barrier for even novice hackers to launch complex attacks, increasing business risk.

Innovative approaches to cybersecurity

Karthikeyan G., Senior Director, Platform Engineering, from Ascendion stresses the necessity of adopting a Zero Trust framework and integrating a DevSecOps mindset. His approach highlights the importance of embedding security at all levels and the value of collaborative efforts in early threat identification and resolution.

Nilesh Kulkarni, Director of Qlik India, echoes these sentiments, focusing on integrating advanced technologies like AI, ML, and blockchain. His insights underline the necessity of robust threat detection and data integrity measures in a digitally interconnected world.

The role of decentralized technologies

Both Karthikeyan and Kulkarni point to the potential of decentralized technologies, like blockchain, in enhancing cybersecurity measures. These technologies offer added layers of security and transparency, particularly vital in distributed transactions and supply chain operations.

Advanced technologies like AI, ML, and blockchain play a crucial role in enhancing security measures, providing opportunities and challenges in real-time threat detection, and fraud prevention, and ensuring transparency in distributed transactions.

Strategic imperatives for cybersecurity

The collective wisdom of these leaders converges on several key themes: the critical role of advanced technologies, the shift from traditional security paradigms to holistic approaches, and the necessity of comprehensive cybersecurity strategies.

Their insights reflect the evolving complexity of cyber threats and the imperative for organizations to adopt multifaceted, innovative strategies. This involves defending against threats and leveraging security as a driver for organizational efficiency and integrity.

Looking ahead: The future of cybersecurity

The cybersecurity landscape appears increasingly complex and demanding as we move forward into 2023 and beyond. The rise of sophisticated cyber-attacks and the evolving nature of threats necessitate a dynamic and forward-thinking approach. Organizations must adopt the latest technologies and foster a culture of security awareness and resilience.

The insights from these industry leaders serve as a beacon, guiding businesses in their quest to navigate this challenging landscape. It's a call to action to embrace innovative, integrated, and comprehensive security strategies to protect against the digital world's sophisticated and rapidly evolving cyber threats.

In conclusion, International Computer Security Day 2023 is a stark reminder of our collective responsibility to safeguard the digital frontier. The insights shared by Swaine, Karthikeyan, and Kulkarni underscores a pivotal moment in cybersecurity, calling for a unified approach in adopting cutting-edge, holistic, and strategic measures in this ongoing battle againIn conclusion, International Computer Security Day 2023 is a stark reminder of our collective responsibility to safeguard the digital frontier. ■

AI & Its Implications On Information Security

While AI has the potential to enhance security measures through threat detection, anomaly identification, and rapid response, it simultaneously presents new challenges.

By **Samrat Bhatt** | editor@cioandleader.com

Artificial intelligence, often abbreviated as AI, represents the forefront of technology's quest to replicate human-like thinking in machines. It aims to imbue computers and systems with the capacity to perform tasks that we commonly associate with humans, like intelligence and decision-making.

AI, the 'X' factor behind security researchers and attackers, will pave a unique future for InfoSec researchers/practitioners and malicious actors. The cyber threat landscape is expected to be significantly impacted by the proliferation of AI. While AI has the potential to enhance security measures through threat detection, anomaly identification, and rapid response, it simultaneously presents new challenges. AI is a weapon; would it be used to guard or rob us depending on who's using it, a security professional or an attacker?

Cybercriminals are increasingly leveraging AI to create sophisticated and evasive attacks. These AI-driven threats can autonomously adapt, discover vulnerabilities, and exploit them unprecedentedly.

As a result, the battle between AI-driven security and AI-driven cyber threats is poised to intensify, ushering in an era of constant technological evolution and vigilance in the cybersecurity domain.

Let's focus on some of the top potential tactics that attackers may employ in 2024 utilizing AI; it is essential to note that cybersecurity professionals and organizations are actively working to counter these threats. Here are some scenarios to consider:

- **AI-enhanced attack automation:** Attackers can leverage AI to automate various stages of attacks, from reconnaissance and vulnerability scanning to exploitation. AI-driven bots can continuously scan the internet for vulnerable targets and launch attacks autonomously, significantly increasing the scale and frequency of attacks.
- **Advanced phishing and social engineering:** AI-powered spear phishing attacks become more sophisticated and convincing. Attackers can create highly personalized messages and mimic trusted contacts or authority figures, making it challenging for targets to discern the deception.
- **AI-generated malware:** Malware authors may use AI to generate polymorphic malware that constantly changes its code to evade traditional signature-based antivirus solutions. AI can also be employed to improve the delivery and execution of malware, making it more effective and challenging to detect.
- **Deepfake impersonations:** Attackers could create deepfake audio and video content to impersonate key figures or executives within organizations. Such deepfakes could be used in social engineering attacks, insider threats, or extortion attempts.
- **AI-powered reconnaissance:** AI can be employed for more efficient surveillance. Attackers may use AI to mine open-source intelligence, social media, and publicly available data to gather information about potential targets and identify vulnerabilities.
- **Exploiting AI-based security tools:** Attackers may target AI-based security solutions, attempting to deceive or bypass them. For instance, they could use adversarial attacks to fool AI-driven anomaly detection systems.
- **AI for evasion and camouflage:** AI can help attackers evade detection by identifying security patterns and finding weaknesses in security measures. Attackers can use AI to camouflage their malicious activities as legitimate traffic or behaviors.
- **Quantum computing threats:** While not AI-specific, attackers may exploit emerging quantum computing capabilities to crack existing encryption methods and undermine data security.

The battle between AI-driven security and AI-driven cyber threats is poised to intensify, ushering in an era of constant technological evolution and vigilance in the cybersecurity domain

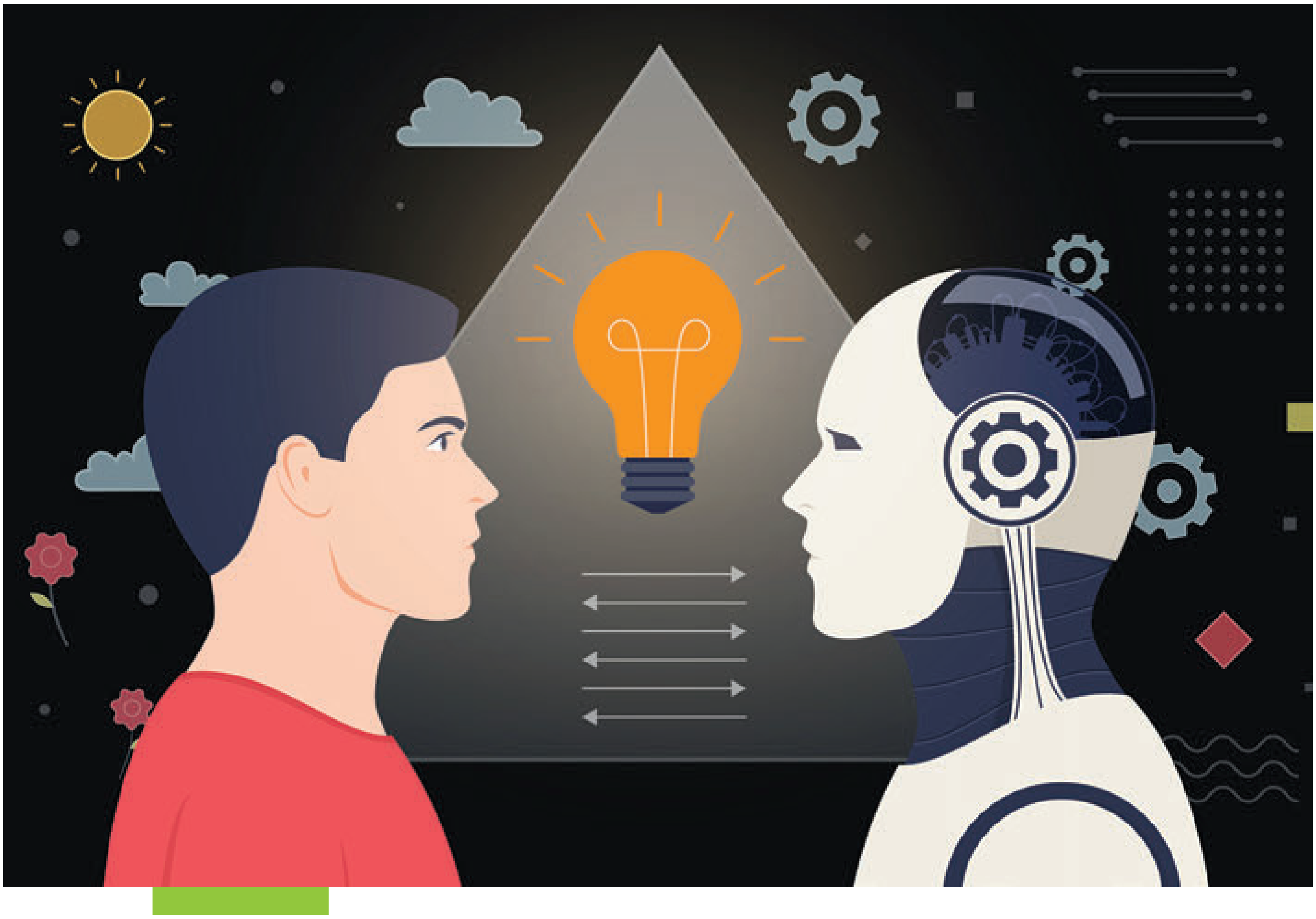
AI can be a powerful tool for attackers and defenders, but proactive defense and threat detection can help mitigate the risks associated with the changing cyberthreat landscape. AI will be pivotal in enhancing security measures and combating emerging threats. Here are some scenarios to consider:

As we depend more on AI, it's crucial to understand and tackle misinformation with AI, while maintaining transparency and focusing on human values..

- **Advanced threat detection and response:** AI-driven security solutions will provide real-time threat detection and response. Machine learning algorithms will continuously analyze network traffic, identifying and mitigating anomalies and threats more effectively than traditional methods.
- **AI-powered security analytics:** Security analysts will rely on AI-driven analytics to rapidly process vast amounts of data. This will help identify patterns and anomalies, enabling proactive threat hunting and faster incident response.
- **Autonomous security systems:** Security systems will become more autonomous with AI. They will automatically respond to threats, isolate compromised systems, and initiate recovery procedures, reducing the required response time and human intervention.
- **Threat prediction and prevention:** AI will be used for predictive analysis, enabling security professionals to anticipate potential threats and vulnerabilities. By analyzing historical data and emerging trends, AI can help organizations bolster their defenses before attacks occur.
- **AI for insider threat detection:** AI will assist in identifying insider threats by analyzing employee behavior and identifying unusual patterns. This will help in detecting malicious or inadvertent insider activities.
- **Quantum-safe cryptography:** As the advent of quantum computing threatens current encryption methods, AI will aid in the development and implementation of quantum-safe cryptography to protect sensitive data.
- **AI-enhanced phishing detection:** AI-powered solutions will provide more robust protection against attacks. They can analyze email content, sender behavior, and other factors to identify phishing attempts more accurately.
- **Advanced access control:** AI will improve access control systems, providing more dynamic and adaptive authorization based on user behavior and context, enhancing security while maintaining user experience.

Artificial Intelligence (AI) represents a transformative force in information processing, enabling the unprecedented handling of vast data sets. Yet, this power also can magnify the spread of misinformation when not adequately controlled. The solution lies in harnessing AI's capabilities to counter its vulnerabilities. As our reliance on AI deepens, it is paramount to grasp the intricacies of misinformation dissemination, employ AI-driven strategies to combat it effectively, and uphold transparency and human-centric values in applying this influential technology. In this ever-evolving landscape, adapting our approaches to tackle misinformation is essential, ensuring responsible AI usage and fostering a trusted digital environment. ■

Samrat Bhatt is a Sr. Director of Information Security at MatchMove India.



Humans Vs. Computers: Automation And Emotional Intelligence

Computers and robots with artificial intelligence can use emojis, but they can't truly understand and express emotions as humans can.

By **Kanu Ratan Butani** | editor@cioandleader.com

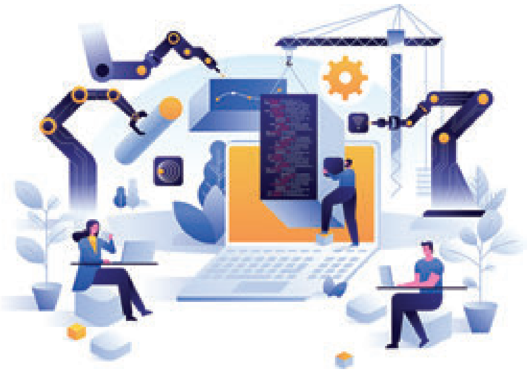
In today's world, computers have become very smart and can do many things by themselves. This is known as automation, and it's like magic! Computers and machines can do repetitive and hard work that used to be done by people. For example, in construction and building, they can carry heavy things and dig the ground quickly. This helps people do more interesting and smart tasks.

However, the world doesn't stay the same all the time. Every day is new, and humans are always looking for new ideas and ways to work. Scientists and researchers are always thinking of new things. Humans have a special ability to create something new, and computers can't do that. Computers, with their artificial intelligence, can learn from existing knowledge, but they can't come up with entirely new things.

Think about emojis, those little symbols we use to show our feelings. There are hundreds of emojis, but humans don't rely on emojis alone to express themselves. Our moods and emotions change, and our faces show it. Computers and robots made with artificial intelligence can't capture these changes. When we look at a person, we can see their mood, how they behave with different people, and how they express their emotions. They act differently with friends, family, and coworkers. If someone upsets them, they might get angry, and their emotions change. But if you say the same thing to a robot, it won't change its emotion or facial expression with every different person. Their expression would be the same with a co-worker and a manager. This is where we see the difference between human emotional intelligence and artificial intelligence in robots.

Automation and computers

Automation is like a superpower for computers. They can do tasks over and over again without getting tired. For example, in construction and civil engineering, computers and machines can carry heavy things to the top floor of a building. They can also dig holes in the ground quickly and easily. This means that human workers can focus on more interesting and important tasks, like planning and supervising the work. Automation has made many jobs easier and faster.



But humans are special

Even though computers are great at automation, they can't come up with new ideas on their own. Humans are unique because they have the power to think creatively. They can imagine new things, create art, and come up with new solutions to problems. Computers can only do what they are programmed to do. They learn from existing knowledge but can't think outside the box.

Emojis and emotions

Emojis are cute little symbols we use in our messages to show our feelings. However, humans don't rely solely on emojis to express their emotions. We have a wide range of emotions, and our faces can show them. When we're happy, our faces light up with smiles. When we're sad, our expressions change. Computers and robots with artificial intelligence can use emojis, but they can't truly understand and express emotions as humans can.

Human behavior

Humans are complex. How we behave and express ourselves depends on many things. We act differently with our friends than we do with our parents or colleagues. If someone upsets us, our reaction depends on who they are. For example, if a friend tells us we're not doing any work, we might not get too upset. But if our boss says the same thing, we might feel very different. We adjust our behavior and emotions based on the people we interact with.

Conclusion

In the world of automation, computers have become incredibly powerful and can perform many tasks efficiently. However, the unique ability of humans to think creatively and generate new ideas is something that sets us apart. Computers are limited to what they have learned from existing knowledge and cannot innovate like humans.

When it comes to emotions and behavior, humans are far more complex and expressive than computers or robots. Our ability to adapt our emotional responses based on the situation and the people we interact with is a testament to the depth of human emotional intelligence. In the end, the blend of human creativity and emotional intelligence remains unmatched in the world of artificial intelligence and automation. ■

—Kanu Ratan Butani is a Senior Manager atAtos Eviden India.

Understanding The Digital Age: Cybersecurity, Privacy, And Data Protection

Improving communication between IT and senior management and focusing on employee training is key to strengthening cybersecurity.

By **Nisha Sharma** | nisha.sharma@9dot9.in

The digital age presents both opportunities and challenges in cybersecurity. As connectivity increases, so does the vulnerability of systems, data, and infrastructure. As we observe Cyber Security Awareness Month, it's essential to understand the integral role each individual and organization plays in bolstering cyber defenses. This article delves into insights from industry leaders, highlighting the path IT leaders should consider for a secure digital future.

The widespread impact of personal cybersecurity decisions

Visionet's Vice President & Head of Cloud & Infrastructure Delivery, Bijo Chacko, underscores the essence of this year's theme, 'Cyber Safety Starts With YOU.' He fluently remarks, "In this era of interconnectivity, our online choices shape our personal cybersecurity and have a ripple effect across the digital network, impacting the collective safety of the online world. Empowerment starts with awareness."

Chacko's statement brings to light the streaming effect individual actions have, reinforcing the idea that a single click or a secure password choice can be the difference between a secured and compromised system. His emphasis on simple but crucial practices, like cautious email handling and responsible online behavior, serve as a potent reminder for IT leaders about the importance of fostering a culture of cyber awareness.

Organizational resilience in an inter-connected era

The conversation shifts gears when looking at the broader organizational framework. **Samir Kumar Mishra, Director of Security Business at Cisco for India & SAARC**, talks about the readiness gap that businesses face today. "A Cisco study indicates that only 24% of organizations in India have the mature level of readiness needed to be resilient against today's modern cybersecurity risks," he states. While the figure is alarming, Mishra's words bring hope. He underscores Cisco's belief that security is, indeed, a collective responsibility. Cisco's vision champions the integration of cutting-edge technologies and expertise to construct resilient security architectures that empower individuals and protect organizations.

The DPDP ACT 2023 calls for seamless security and enhanced cybersecurity education to empower users.

The hybrid world we operate in demands a comprehensive understanding of the network's nuances. Mishra rightly says, "If a device is connected, it needs to be protected." For IT leaders, this reiterates the importance of an all-encompassing approach, integrating both point tools and platforms to achieve resilience without complicating the security infrastructure.

Ripu Bajwa, Director and General Manager of Data Protection Solutions at Dell Technologies India, posits, "In this age of connectivity, where the internet has become an integral part of our daily existence, protecting our online privacy is paramount. As a country progressing rapidly towards a digital future, we need to respect and understand the significance of preserving the privacy and security of our personal data."

DPDP Bill 2023

With the introduction of the Data Protection Bill 2023 in India, the emphasis on cybersecurity has peaked, urging organizations and individuals to be more vigilant than ever.

Guardians of cyber trust

Mr. Joy Sekhri, Vice President, Cyber & Intelligence Solutions, South Asia, Mastercard, stresses the non-negotiable essence of cybersecurity and data privacy. He said, "Protecting sensitive information, both customer and internal, is not just a legal requirement but a fundamental trust-building measure." The risks of cyberattacks are multi-dimensional, spanning financial losses, reputational damage, and more. Sekhri emphasizes that protecting data is about maintaining the trust of stakeholders and ensuring the integrity and confidentiality of operations. On the preventative side, investments in encryption, multi-factor authentication, and regular security audits are indispensable. Collaborative approaches, staying abreast of threats, and adhering to industry standards remain pivotal.

On the verge of a cyber-resilient world

Venkatesh Subramaniam, Cybersecurity and Privacy Head at Mindsprint, drives that cybersecurity isn't just an IT issue—it's a brand differentiator and an enabler for businesses. He underlines the importance of adopting a security-by-design mindset in an age where AI, IoT, and Cloud drive innovations. Subramaniam praises the Data Protection Bill 2023, emphasizing that it symbolizes both an opportunity and a collective responsibility. "We must ensure frictionless security and promote cybersecurity education to empower our users."

Navigating the digital defense landscape

Madhusudan Krishnapuram, Vice President of Engineering and Managing Director, India at GoTo, emphasizes shared responsibility for cybersecurity. "It is imperative for businesses to prioritize cybersecurity awareness and invest in technologies such as Zero Trust Network Architecture." He believes in fostering a cybersecurity culture that starts with simplification, arming IT leaders with tools to navigate the intricate world of digital defense.

A clarion call to 'secure the world'

Aladdin Elston, Head – Information Security at Altimetrik, paints a stark picture of the growing cyber threats, with India witnessing an alarming rise in attacks. He sees the Data Protection Bill 2023 as a significant move towards shielding data. Yet, Elston emphasizes that the task isn't solely technological—it's a collective endeavor. "The formidable task of thwarting cyber threats can be overcome with a highly skilled team of cybersecurity professionals."

Towards a proactive cybersecurity stance

Balaji Rao, Area Vice President, India & SAARC, at Commvault, comprises the significance of Cyber Security Awareness Month. He speaks to the evolution of cyber threats and highlights the need for a proactive approach. "Enterprises must shift from a reactive to a proactive approach towards cybersecurity." Rao believes in the potential of new-age technologies like AI in early threat detection and emphasizes the value of automation in cybersecurity processes.

Data storage and recoverability

While privacy remains a cornerstone, the dialogue in cybersecurity is rapidly evolving, with an increasing emphasis on data storage and recovery. Mr. Sandeep Bhambure, Managing Director and Vice President for India & SAARC at Veeam Software, reminds us of the gravity of the situation, "Data breaches are not only a threat towards reputation, but attackers can also encrypt data, making it unrecoverable. Businesses should no longer think 'if we get hacked' but rather, 'when we get hacked, what is our recovery plan?'"

Veeam's recent report points to a rising trend in cybersecurity investments across the Asia Pacific. However, mere investment isn't the panacea. As Bhambure aptly points out, bridging communication gaps between IT and senior management, coupled with an emphasis on employee upskilling, is essential to fortifying cybersecurity strategies. Having a proactive business continuity plan, choosing the right backup solutions, and constantly evaluating new technologies will be pivotal in navigating potential cyber threats.

Conclusion

In assessing the perspectives provided by industry leaders, it's evident that the cybersecurity landscape in the digital age is multifaceted, requiring attention at both the individual and organizational levels. Individual actions in the digital space have cascading effects on broader systems, emphasizing the importance of personal cybersecurity awareness. Organizations, on the other hand, face a readiness gap, with many not adequately prepared for modern cyber threats. The introduction of the Data Protection Bill 2023 highlights the legislative emphasis on cybersecurity, but it's equally crucial for organizations to internalize this emphasis and integrate it into their operations. The dual focus on data protection and recovery underscores the importance of having both defensive and responsive measures in place. Collaboration, a shift from reactive to proactive strategies, and continuous education and upskilling are all integral components of a robust cybersecurity approach. The insights provided reaffirm that while technology plays a pivotal role in cybersecurity, the human element remains at the core of building a secure digital future. ■

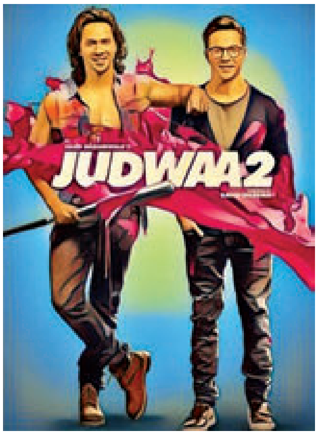
2024 -of tech trends, CIO choices, and Bollywood

The CIO's focus: beyond tech, to deliver outstanding experiences by understanding the needs of customers, employees, and partners.

By **Deepak Bhosale** | editor@cioandleader.com

The beginning of a new year is a great opportunity to reset your thinking and plans, and hence, this post may be of help. The year 2023 saw one of the most disruptive technologies (Chat GPT) take the world by storm and with the potential to impact our lives like never before. I guess we have more in store. Here are a few tech trends that may be some fodder for thought for the CIOs / Professionals to consider as they plan for 2024. And since you can't take the Bollywood out of me, I have used it metaphorically for easy recall 🙂

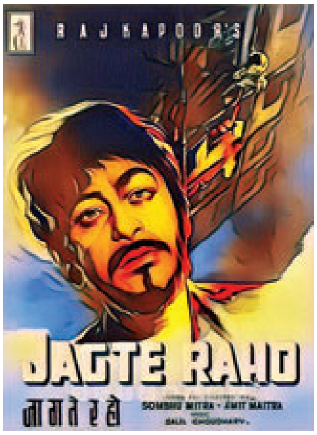
TWINNING OF BUSINESSES



The ease with which one can acquire IT and OT feeds/data points leverages the power of cloud computing. Adopting 5G technologies and building visual analytics makes digital twins a MUST-DO in the CIO's List. 2024 will see a rapid increase in the growth of digital twins of assets, manufacturing facilities, stores, and maybe even consumers.

These (JUDWAs) twins are going to drive better and smarter business decisions. I have seen manufacturing teams test the hypothesis in the digital twin and execute it in the physical one. This has led to a reduction in manufacturing cycle times, better equipment maintenance, and near-zero defects in products. The CIO needs to make an assessment of the data points available, evangelize Digital twins with the manufacturing heads, and create a plan to generate value.

SECURITY never SLEEPS



CIOs/CISOs are going to see one of the most challenging years. Post-COVID, the CIOs are left with hybrid infrastructures to support WFH/WFO, which in itself creates few risks. With lines blurring between IT and OT, Ransomware attacks becoming easy, AI getting used to engineer attacks, and deep fakes becoming increasingly deceptive, there is a lot at hand to manage

A CIO/CISO needs to keep assessing the organization's security posture on a regular basis, benchmark with the industry best, and create a plan to be there. CISOs in progressive organizations are budgeting a minimum of 15% of their IT spending on security. However, CIOs, beware: this is a year wherein we will see a lot of news related to confidential data getting stolen. It continues to be "Jagte Raho" times for CISOs.

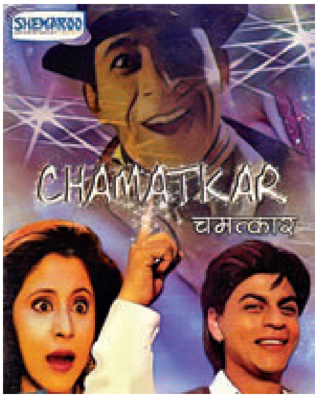
EXPERIENCES create the MAGIC

The CIO needs to anchor all work done on creating winning experiences that can be delivered to the stakeholders, may it be for customers, employees, or business partners. This is not a technology problem.

Delivering great experiences will depend on the IT team's ability to empathize with the customer/ partner/employee challenges. The customer-centric IT outfits spend a minimum of 10% of their time in the market. The CIO has to take accountability for creating seamless, contextual, and personalized phygital journeys. AI driven Omnichan-

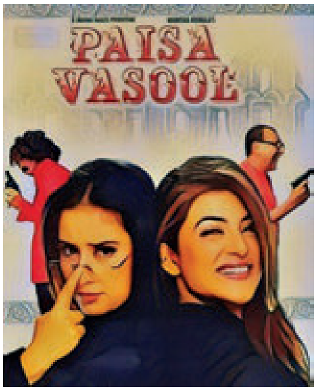
The CIO must evaluate available data, promote Digital Twins among manufacturing leaders, and devise a plan to create value.

nel experiences in 2024 will be in focus. I clearly see Customer Data Platforms (CDP) becoming mainstream technology to drive magical experiences. This is the year wherein the CIO can be a cause in creating "Chamatkar" (Magic) for all stakeholders



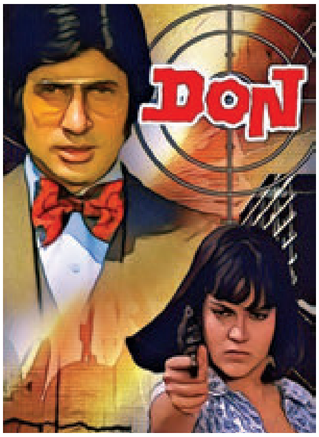
BUSINESS Value of IT

The demands on the IT teams to drive technology-enabled transformation are going to be far higher than before in 2024 and will continue to rise. The funding also will come more willingly than before. The CIOs can bucketize the investments into operational, transformational, and disruptive. However, a stronger onus (Paisa Vasool) to justify the value will come in. The CIO needs to have a business-aligned framework to measure, monitor, and communicate the business value of IT. Progressive CIOs will take the bold step of adopting KPIs for themselves, which will be around generating a certain value (Additional revenues or Lower costs) through cutting-edge technology. As a CIO, are you considering a KPI of 5% of your Net Sales generated through Algorithms?



The new DONS

The hyper-scalers and cloud service providers are soon becoming the new DONs. The cloud is not just a disruptive technology but has now become more of a business necessity. The integration of AI and ML, the rise of edge computing, the prevalence of multi-cloud & hybrid environments, and the advancement of Infrastructure as a Code (IaC) are the defining trends.



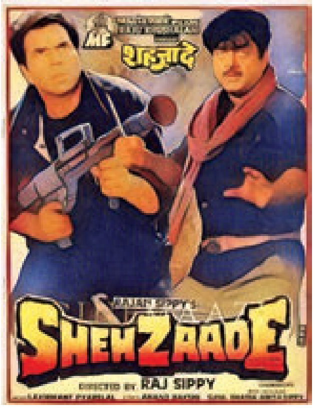
Progressive CIOs will adopt bold KPIs focused on generating value, like increasing revenue or reducing costs, through advanced technology.

Organizations seeking for agile innovation and finding it difficult to manage skills have started aggressively moving on to the cloud. I foresee a large number of business-critical applications like ERPs going to the cloud. CIOs need to understand the shifts from Capex to Opex and create an organization-specific strategy for modernizing and sustaining the IT landscape.

The NEW KIDS on the BLOCK

CIOs need to keep tracking the new kids on the block. Gen AI came in like a crown prince (Shehzada) last year. As a CIO, if you have not started Pilots of any sort on Gen AI, then I guess you are about to miss the train of exponential transformation.

You will need to plan in a manner to ensure atleast 4-5 use cases into production in 2024. These experiences and learnings will help the CIO plan a more solid strategy for Gen AI. As a CIO, you will need to keep an eye on the other Shehzades who are in the making, namely Quantum computing, Autonomous intelligence, blockchain, Extended reality/Wearables, AI Augmented Development, Platform Engineering, and Sustainable systems.



It's a bit of a challenge to cover the details of tech trends. Maybe you can put your insights in the comments and build on this content. Thanks in advance for that. ■

—Deepak Bhosale is an AVP at Asian Paints.

To follow the latest in tech,
follow us on...

facebook.com/digitgeek

digit.in/facebook

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

नयी स्टोरीज़
हुवावे ऑनर 6 स्मार्टफ़ोन: रु. 20,000 की रेंज में बेहद उम्दा फ़ोन
digit.in हिंदी
गैजेट और टेक्नोलॉजी न्यूज़

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

डिजिट

@DIGIT.IN

FOLLOW US ON

Instagram

FOR THE LATEST UPDATES IN TECH

digit.in

digit.in

2,988 Posts

120K Followers

72 Following

Digit

Digital creator

Digit is the largest online personal technology community in India. Welcome to the world of Digit!

Your Technology Navigator since 2001.

www.linktr.ee/digit.in

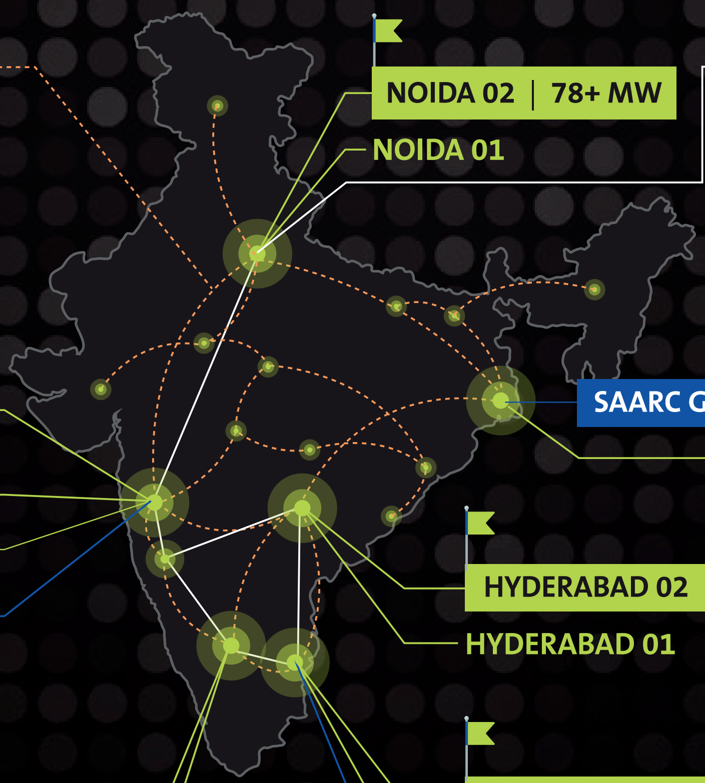
Following

Message

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

sify

Empowering India’s Digital Backbone



Metro Networks
36000+Kms of Fiber access
5000+ Connected Buildings
65+ Interconnected DCs

NOIDA 02 | 78+ MW

NOIDA 01

Express Long Haul
Backbone, High Bandwidth
and Low Latency
across Key Locations

MUMBAI 03 RABALE
200+ MW

MUMBAI 02 AIROLI

MUMBAI 01 VASHI

CLS, Versova, Mumbai

SAARC Gateway, Kolkata

KOLKATA 01

HYDERABAD 02 | up to 250+ MW

HYDERABAD 01

CHENNAI 02 | 78+ MW

CHENNAI 01

CLS, Siruseri, Chennai

BENGALURU O2 | 22+ MW

BENGALURU 01

Sify has built 11 data centers with 100+ MW of IT power and will expand to 350+ MW by 2025. Committed to sustainability, Sify has already commissioned 200+ MW of renewable energy. We continue to invest in AI/ML led automation, green initiatives, RAS-based design infrastructure, interconnected ecosystems, advanced security and hybrid/multi-cloud solutions to enhance India's digital infrastructure and strengthen the nation's digital backbone.

Tried. Tested. Trusted.

Your Digital Infrastructure Partner for over 23 years

Digital Network
Infra Services

Digital Data Center
Infra Services

Network Digital
Services

Cloud & IT
Managed Services

Digital Security
Services

Full Stack
Observability

Digital Apps
Services

Industry Apps
Services

BOOKINGS
OPEN