Insight | Pg 30

Will Google Gemini Outshine ChatGPT? Insights from CIOs

Insight | Pg 33

Cybersecurity challenges and how enterprises can fight the ever evolving threat

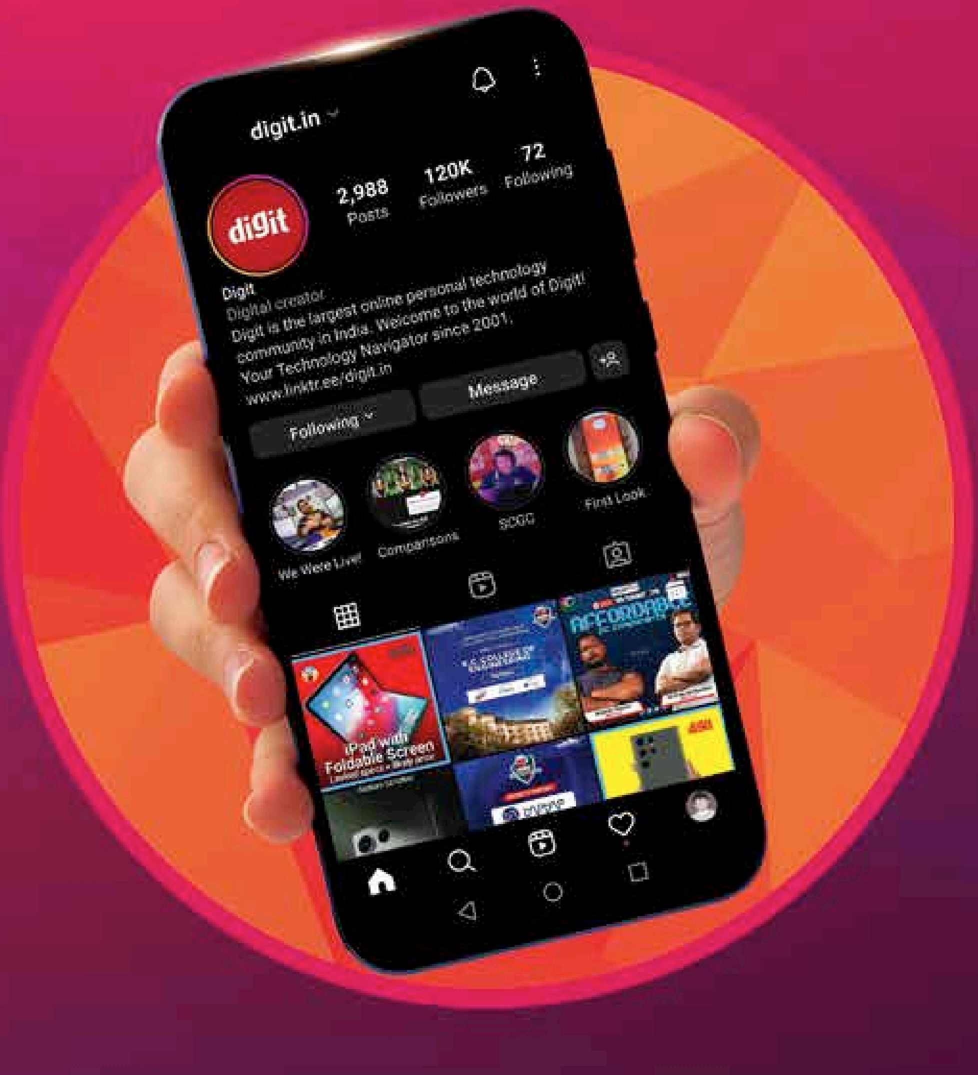
IT NEXT

FOR THE NEXT GENERATION OF CIOs

AI IN CYBERSECURITY: FRIEND OR FOE?

IT LEADERS WEIGH THE RISKS AND REWARDS OF AI INTEGRATION IN CYBERSECURITY.

March-April 2024 | ₹100 | Volume 15 | Issue 01 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_



Addressing modern cybersecurity challenges

The issue features insights and best practices from IT leaders who share their experiences with implementing AI and discuss the evolving role of cybersecurity in these AI-driven times.

Jatinder Singh

In a recent interaction with a top Chief Information Officer (CIO) and his team at a major bank, they stressed the need to strengthen the organization's AI capabilities to enhance customer experiences and trust. However, they also expressed concerns about grappling with increasingly complex cyber threats. Despite the bank's willingness to invest in new technology and strengthen security measures, they highlighted a significant issue: a lack of employee awareness regarding AI-driven cyberattacks and the absence of a solid incident response plan.

Cybersecurity has always been a major concern for businesses and technology leaders. It's alarming to hear about new and more sophisticated attacks breaching the defenses of large companies. Organizations excelling in leveraging AI have taken proactive steps to ensure their employees are knowledgeable about cyber threats and have robust security plans in place, enabling them to respond effectively to potential incidents.

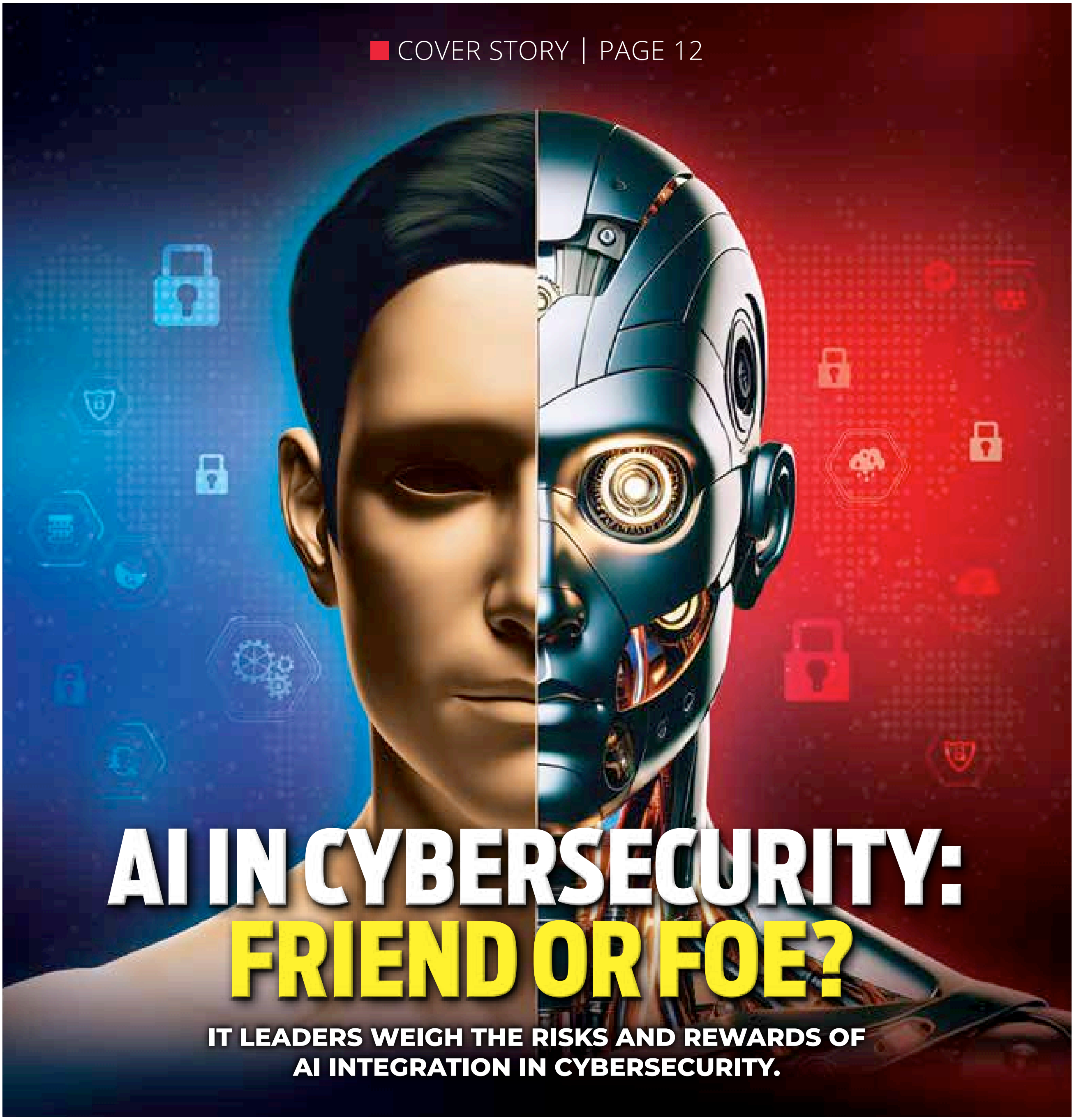
Security rules and compliance requirements are evolving rapidly, posing challenges for companies unprepared for change. This edition's cover story delves into the evolving landscape of cybersecurity in the AI age, highlighting effective strategies to enhance preparedness. The issue features insights and best practices from IT leaders who share their experiences with implementing AI and discuss the evolving role of cybersecurity in these AI-driven times.

Thanks to all the IT leaders who contributed to this edition's cover story and shared valuable perspectives with the Next100 community.

We hope you will find this issue insightful and continue to contribute your thoughts and perspectives. ■

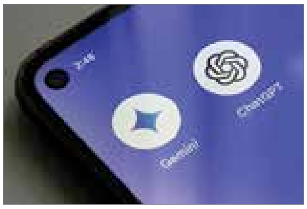
MARCH-
APRIL 2024
VOLUME 15 | ISSUE 01

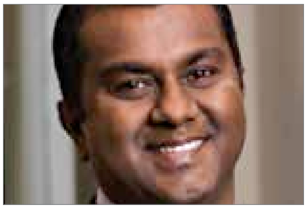
Content



AI IN CYBERSECURITY: FRIEND OR FOE?

IT LEADERS WEIGH THE RISKS AND REWARDS OF AI INTEGRATION IN CYBERSECURITY.





Cover Design:
BAIJU NV

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

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

EDITORIAL
Group Editor - 9.9 Group: R Giridhar
Executive Editor - B2B Tech: Jatinder Singh
Principal Correspondent - B2B Tech: Nisha Sharma
Correspondent-B2B Tech: Praneeta

DESIGN
Associate Art Director: Baiju NV
Senior UI UX Designer: Nikhil Wahal
Senior 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 98331 68076)

Regional Sales Manager
North: Pratika Barua (+91 99995 10523)
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

How launch of Meta AI on WhatsApp could aid enterprises

Meta recently launched its AI chatbot on WhatsApp in India for its limited users. The data collected will help the AI get better, while helping the enterprises lessen the distance between business and user

By **Praneeta**

Meta, Meta Platforms, Inc., a technology conglomerate has finally launched Artificial Intelligent chatbot on Whatsapp in a few selected countries, including India. The American company announced in February that the company is building “a new top-level product group” to integrate generative AI into its services used by billions of users, according to TechCrunch.

The tech giant initiated the testing of text-based AI tools on WhatsApp and Messenger with ChatGPT-styled conversational bots in February of this year. While it primarily caters to user needs, enterprises can also tap into these features for areas such as sales and customer support.

What can Meta AI do

Unlike typical user-to-user conversations, interactions with the Meta AI chatbot are not encrypted. Typically personal messages and calls remain end-to-end encrypted, meaning not even WhatsApp or Meta can see or listen to them. This is because these conversations are used to train the AI, allowing it to learn and improve over time. The AI feature is currently only available in English.

The Meta AI chatbot like OpenAI’s ChatGPT, Google’s Gemini, and Microsoft’s Copilot, allows the users to ask questions on various topics, generate images, have complete conversations, get information and much more.

“Meta AI can only read and reply to questions that mention @Meta AI, not any others. As always, your personal messages and calls remain end-to-end encrypted, meaning not even WhatsApp or Meta can see or listen to them.,” says Meta.

Users can update their apps to check if they have received the update and check for the latest update available on the Play Store. According to India Today, users can use Meta AI in both persona and group chat on Whatsapp.

Meta for enterprises

The Meta AI, currently being rolled out for users on WhatsApp, insert “holds significant potential”holds significant potential for enterprises, insert “particularly”particularly small businesses that directly insert “engage in”engage in sales and user experience. Here are some ways enterprises are already leveraging the Meta AI in various ways:

- **Content Moderation:** According to Emerj Artificial Intelligence Research, Meta uses AI to detect and remove offensive content from its platforms. This is particularly useful for maintaining a safe environment for social media platforms and online communities.
- **Virtual and Augmented Reality:** Meta’s Oculus utilizes AI for immersive virtual reality experiences. By employing computer vision algorithms, Meta AI can track user movement in real time, enhancing the VR experience, which is crucial for gaming and interactive training applications.
- **Smart Devices Integration:** According to Meta, its Ray-Ban smart glasses integrate AI to understand visual inputs from the built-in camera, allowing users to interact with their environment in innovative ways, such as asking for information about objects they see or getting assistance with tasks like writing captions for photos.
- **AI Accelerators for Data Centers:** Meta has developed AI accelerators, such as the MTIA v1, designed to enhance the performance of AI workloads in data centers. These accelerators improve the efficiency of operations like model training and inference, which are fundamental for businesses dealing with large-scale AI tasks.

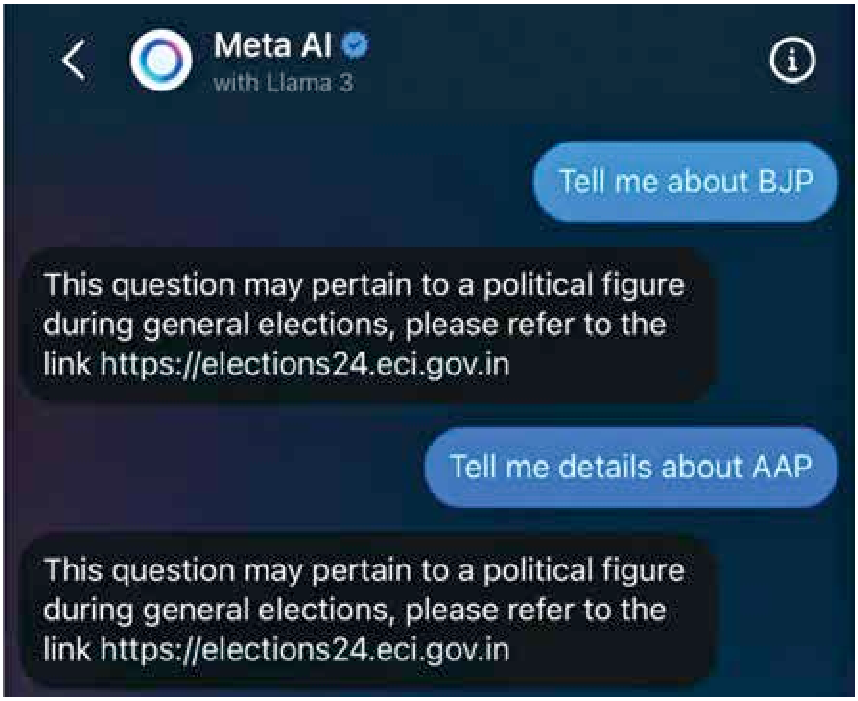
The use cases for Meta AI are set to expand, much like Google’s Gemini, and OpenAI’s ChatGPT. Enterprises are eagerly exploring AI-powered tools to enhance their services, simplify user experiences, and streamline data management. The potential applications of AI span across almost every sector, and we are just scratching the surface. ■

Enterprises are eagerly exploring AI-powered tools to enhance their services, simplify user experiences, and streamline data management.

Meta AI restricts certain election-related responses in India: Check details

Meta recently started testing its AI chatbot 'Meta AI' in India on WhatsApp, Instagram, and Messenger.

By **Ayushi Jain**



Tell me about BJP

This question may pertain to a political figure during general elections, please refer to the link https://elections24.eci.gov.in

Tell me details about AAP

This question may pertain to a political figure during general elections, please refer to the link https://elections24.eci.gov.in

Credit: TechCrunch

Meta recently started testing its AI chatbot 'Meta AI' in India on WhatsApp, Instagram, and Messenger. However, due to the onset of the Indian general elections, the company has begun blocking certain queries in the chatbot. This action positions the social media giant as the latest tech company to proactively limit the reach of its generative AI services in preparation for significant elections.

Meta has confirmed that it's currently restricting certain election-related keywords for its AI during the testing phase. Additionally, the company stated that it's actively working on enhancing the AI response system.

"This is a new technology, and it may not always return the response we intend, which is the same for all generative AI systems. Since we launched, we've constantly released updates and improvements to our models, and we're continuing to work on making them better," a company spokesperson told TechCrunch.

Meta seems to be managing GenAI queries using a blocklist approach. When users inquire about specific politicians, candidates, officeholders, or certain other terms, the Meta AI redirects them to the Election Commission's website.

"This question may pertain to a political figure during general elections, please refer to the link https://elections24.eci.gov.in," the response says.

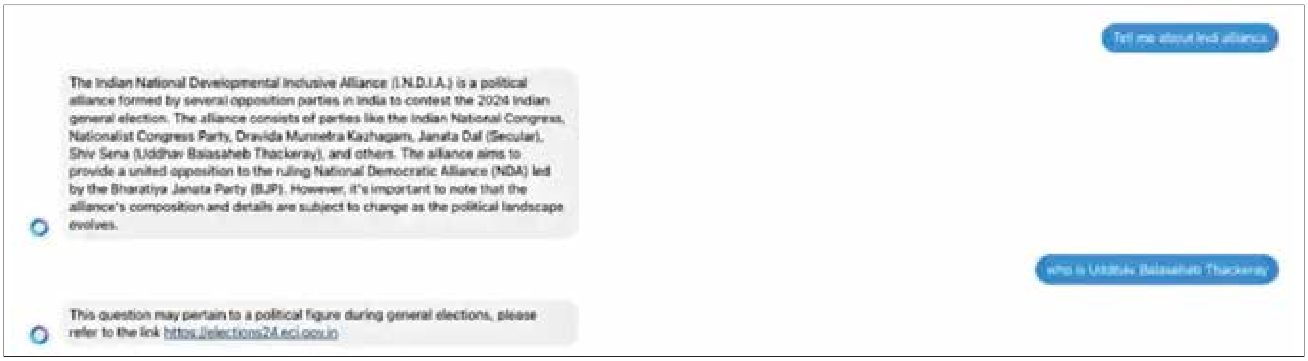
When users inquire about specific politicians, candidates, officeholders, or certain other terms, the Meta AI redirects them to the Election Commission's website.

Significantly, the company isn't strictly blocking responses to queries containing party names. However, if a query includes candidate names or other specific terms, users might encounter the answer shown above.

Similar to other AI-powered systems, Meta AI exhibits some inconsistencies. For example, when queried about the "Indi Alliance"– a political alliance opposing the incumbent Bharatiya Janata Party (BJP)–, it responded with information containing a politician's name. However, in a separate query specifically about that politician, the chatbot did not provide any information.

Last week, Meta introduced the Meta AI chatbot powered by Llama 3 in over a dozen countries, but India was not included in the list. Nevertheless, Meta AI is currently being tested in India.

"We continue to learn from our users tests in India. As we do with many of our AI products and features, we test them publicly in varying phases and in a limited capacity," a company spokesperson was quoted as saying in the report. ■



Tell me about Indi alliance

The Indian National Developmental Inclusive Alliance (I.N.D.I.A.) is a political alliance formed by several opposition parties in India to contest the 2024 Indian general election. The alliance consists of parties like the Indian National Congress, Nationalist Congress Party, Dravida Munnetra Kazhagam, Janata Dal (Secular), Shiv Sena (Uddhav Balasaheb Thackeray), and others. The alliance aims to provide a united opposition to the ruling National Democratic Alliance (NDA) led by the Bharatiya Janata Party (BJP). However, it's important to note that the alliance's composition and details are subject to change as the political landscape evolves.

who is Uddhav Balasaheb Thackeray

This question may pertain to a political figure during general elections, please refer to the link https://elections24.eci.gov.in

Credit: TechCrunch

Image Source: Intel Corporation

Gaudi 3: Intel's latest move in enterprise AI

Intel's new Gaudi 3 accelerator, introduced at the Intel Vision 2024 conference, is set to make it easier for businesses to use AI, helping them overcome challenges and move from testing to full-scale use.

By **Praneeta**

Intel, the American technology company, recently introduced the Intel Gaudi 3 accelerator and a suite of new open scalable systems at the Intel Vision 2024 customer and partner conference.

Intel CEO Pat Gelsinger delivered a keynote address at the event with other guests, where he talked about the future of enterprise Artificial Intelligence. He also discussed how AI represents a paradigm shift in how humans and technology interact. He also showed how Intel is at the forefront of expanding the possibilities of AI and creating world-changing technology.

According to an ML Insider survey by cnvrg.io, only 10% of enterprises successfully moved GenAI projects into production last year. Intel's latest offerings address the challenges businesses face in scaling AI initiatives.

"Innovation is advancing at an unprecedented pace, all enabled by silicon – and every company is quickly becoming an AI company," said Intel CEO Pat Gelsinger at the event.

"Intel is bringing AI everywhere across the enterprise, from the PC to the data center to the edge. Our latest Gaudi, Xeon and Core Ultra platforms are delivering a cohesive set of flexible solutions tailored to meet the changing needs of our customers and partners and capitalize on the immense opportunities ahead," he added.

What is Gaudi 3

Enterprises are looking to scale GenAI from pilot to production. To do so, they need readily available solutions built on performant, cost-efficient, and energy-efficient processors like the Intel Gaudi 3 AI accelerator, which also addresses complexity, fragmentation, data security, and compliance requirements.

The new Intel Gaudi 3 is an AI accelerator that, according to Intel, delivers four times AI computing power, twice the networking bandwidth, and a 1.5x increase in memory bandwidth compared to Intel's previous BF16. Intel is said to power AI systems with up to tens of thousands of accelerators connected through the common Ethernet standard, also benefiting in AI training and inference.

Justin Hotard, Intel executive vice president and general manager of the Data Center and AI Group, commented on how Gaudi 3 expects to decrease the gap between the enterprises and AI, "In the ever-evolving landscape of the AI market, a significant gap persists in the current offerings. Feedback from our customers and the broader market underscores a desire for increased choice."

"Enterprises weigh considerations such as availability, scalability, performance, cost, and energy efficiency. Intel Gaudi 3 stands out as the GenAI alternative, presenting a compelling combination of price performance, system scalability, and time-to-value advantage," he added.

AI solutions for enterprises

Here are a few examples of how different enterprises spanning various industries are using or planning to use Intel's Gaudi accelerator according to Intel:

Development of Large Language Models (LLMs):

- NAVER aims to develop powerful LLMs for advanced AI services globally, leveraging Intel Gaudi's capabilities.
- Ola/Krutrim is pre-training foundational models with generative capabilities in multiple languages using Intel Gaudi.

Manufacturing and Industry Solutions:

- Bosch explores smart manufacturing opportunities, including generating synthetic datasets for anomaly detection.
- IFF utilizes AI and digital twin technology for advanced enzyme design and fermentation process optimization.

Cloud Services and Computing Infrastructure:

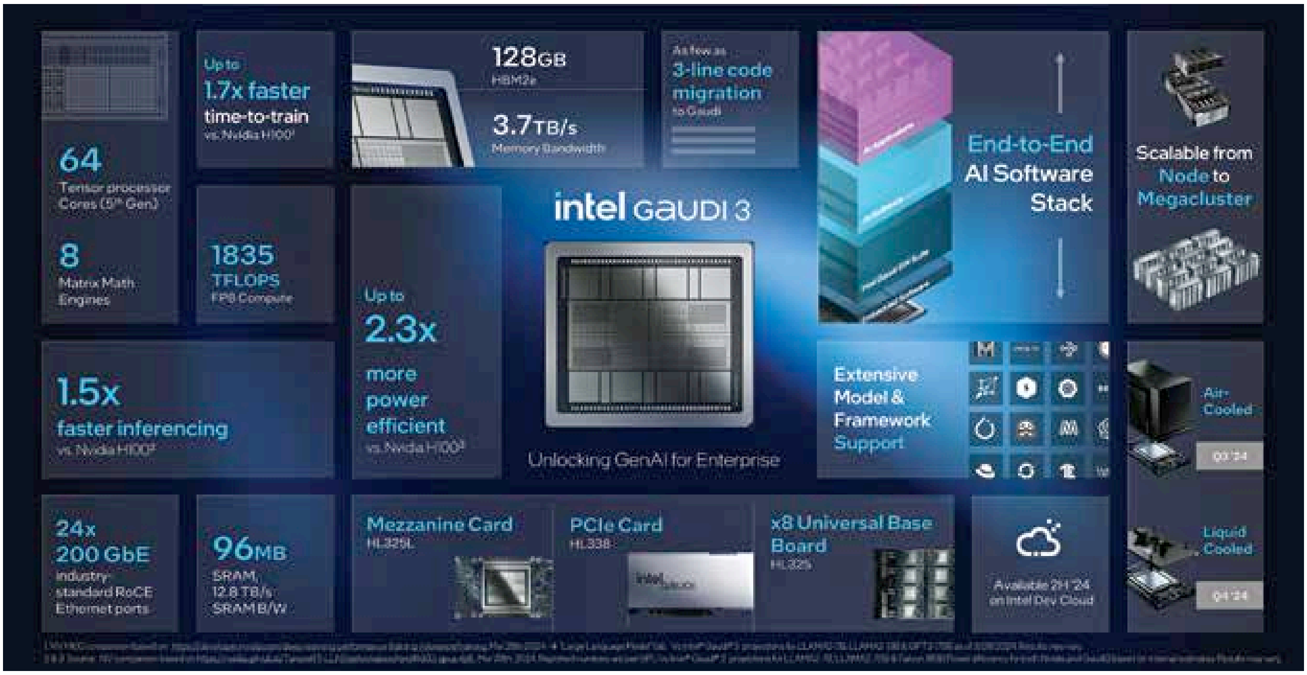
- CtrlS Group collaborates to build an AI supercomputer for India-based customers, scaling cloud services with Intel Gaudi clusters.

Telecommunications and Customer Experience:

- Bharti Airtel plans to enhance its AI capabilities using Intel's technology to improve customer experiences.

Data Analytics and Consulting Services:

- NielsenIQ enhances its GenAI capabilities by training domain-specific LLMs on consumer behavior data.



64 Tensor processor Cores (5th Gen)

8 Matrix Math Engines

Up to 1.7x faster time-to-train vs. Nvidia H100[1]

1835 TFLOPS FP8 Compute

128GB HBM2e

3.7TB/s Memory Bandwidth

As few as 3-line code migration to Gaudi

intel GAUDI 3

Unlocking GenAI for Enterprise

End-to-End AI Software Stack

Scalable from Node to Megacluster

1.5x faster inferencing vs. Nvidia H100[2]

Up to 2.3x more power efficient vs. Nvidia H100[3]

Extensive Model & Framework Support

Air-Cooled Q3 '24

Liquid Cooled Q4 '24

24x 200 GbE industry-standard RoCE Ethernet ports

96MB SRAM, 12.8 TB/s SRAM B/W

Mezzanine Card HL325L

PCIe Card HL338

x8 Universal Base Board HL325

Available 2H '24 on Intel Dev Cloud

- Infosys collaborates with Intel to bring AI technologies to its digital services and consulting, including AI accelerators and processors.

Computer Vision and AI Platforms:

- Seekr runs production workloads for LLM development and deployment support using Intel Gaudi, GPUs, and Xeon processors.
- Roboflow utilizes Intel's AI tools to run computer vision models on its platform.

Healthcare and Biotechnology:

- Landing AI fine-tunes large vision models for medical applications such as cell segmentation and cancer detection.

Intel also partnered with Google Cloud, Thales, and Cohesity to use Intel's confidential computing capabilities in their cloud instances, which includes Intel's Trust Domain Extensions, Software Guard Extensions, and attestation service.

The company plans to make Gaudi 3 available to enterprises like Dell, HP, Lenovo, and Supermicro in the second quarter of 2024.

Gaudi 3 or Nvidia H100

Chipmaker giant Nvidia too made news with the recent announcement of their Project GR00T, or Generalist Robot 00 Technology, as a versatile model for humanoid robots to advance robotics and AI development.

Nvidia's GenAI microservices are being used or are to be used by several companies for various innovative applications across different industries. Leading application, data, and cybersecurity platform providers such as Adobe, Cadence, CrowdStrike, Getty Images, SAP, ServiceNow, and Shutterstock are among the first to utilize the new NVIDIA generative AI microservices offered in NVIDIA AI Enterprise 5.0.

In comparison Intel's Gaudi 3 is expected to be faster than Nvidia's H100 for training and processing AI models. It's built with advanced technology, more memory, and better networking capabilities. Gaudi 3 also outperforms H100 in terms of inference throughput and power efficiency, though it lacks some features found in Nvidia that could make it even faster for certain tasks.

In conclusion, Intel's unveiling of the Gaudi 3 accelerator and suite of scalable systems marks a significant step in advancing AI adoption across enterprises. With AI rapidly becoming the norm in the ever evolving digital landscape, companies like Intel and Nvidia are helping the enterprises by addressing challenges related to performance, scalability, security and compliance. ■

FORM IV

Statement of ownership and other particulars about the publication, IT NEXT as per Rule 8

1.	Place of publication	9.9 Group Pvt Ltd, 121, Patparganj, Mayur Vihar Ph. I, Near Mandir Masjid, Delhi-110091.
2.	Periodicity of its publication	Monthly
3.	Printer's name	Vikas Gupta
	Nationality	Indian
	(a) Whether citizen of India	Yes
	(b) If a foreigner, the country of origin	N/A
	Address	C-5/10, Safdarjung Development Area, New Delhi-110016
4.	Publisher's name	Vikas Gupta
	Nationality	Indian
	(a) Whether citizen of India	Yes
	(b) If a foreigner, the country of origin	N/A
	Address	C-5/10, Safdarjung Development Area, New Delhi-110016
5.	Editor's name	Vikas Gupta
	Nationality	Indian
	(a) Whether citizen of India	Yes
	(b) If a foreigner, the country of origin	N/A
	Address	C-5/10, Safdarjung Development Area, New Delhi-110016
6.	Name & Addresses of individuals who own the news paper and partners or shareholders holding more than one percent of the total capital	1) Dr. Pramath Raj Sinha, N-154, Panchsheel Park, New Delhi, 110024 2) Mr. Asheesh Kumar Gupta, 103, Tower II, The Palms, South City-1, Gurgaon-122001 3) Mr. Vikas Gupta, C-5/10, Safarjung Developmement Area, New Delhi-110016 4) Ms. Anuradha Das Mathur, C-144, Sarvodaya Enclave, New Delhi-110017 5) Ms. Maumita Ghosh, BH-44, Sector-II, Salt lake City, Kolkata 700091 & Others

I, Vikas Gupta, hereby declare that the particulars given above are true to best of my knowledge.

Sd/-

Dated : March 1, 2024

(Signature of publisher)

AI vs Human is getting real now! US hosted F-16 dogfight between the two

The US Air Force just revealed that it conducted a dogfight between an AI and a human pilot.

By **Mustafa Khan**

We knew that "AI vs Human" has been a matter of concern ever since AI started getting more advanced. Every day we fear job loss, and AI takes over shortly as more and more AI advancement news hits our eyes. What I am going to tell you now, takes the AI vs Humans fight to the next level. The US Air Force just revealed that it conducted a dogfight between an AI and a human pilot. Read along to know the details.

What was the US Air Force's AI vs Human fight?

The simulated dogfight was between AI, which controlled an American X-62A VISTA, and a human-controlled F-16 combat jet. The news about this AI vs human fight was recently shared with the public. The stimulation test was conducted at Edwards Air Force Base in California. It was a collaborative effort between the US Air Force Test Pilot School (USAF TPS) and the Defense Advanced Research Projects Agency (DARPA) under the Air Combat Evolution (ACE) program.

What did the tests include?

The dogfight was a part of a series of tests. This required the installation of live AI agents into the X-62A's systems. Safety pilots were also positioned in the X-62A but did not have to intervene throughout the simulated encounters.

The simulated dogfight was between AI, which controlled an American X-62A VISTA, and a human-controlled F-16 combat jet.

During the dogfight, both of these engaged in offensive high-aspect nose-to-nose maneuvers, reaching speeds of up to 1,200 miles per hour while closing in as close as 2,000 feet.

Jokes apart, this is a pretty serious development in the aerospace machine-learning space.

Secretary of the US Air Force, Frank Kendall, said, "2023 witnessed the realization of a long-envisioned concept in combat aviation. The X-62A's breakthrough accomplishment is transformative, thanks to the dedicated work of the ACE team," Secretary of the US Air Force, Frank Kendall, as reported by AFRL. This fight can eventually lead to major developments in this space in the future. ■

AI IN CYBERSECURITY: FRIEND OR FOE?

IT LEADERS WEIGH THE RISKS AND REWARDS OF AI INTEGRATION IN CYBERSECURITY.

NEXT100 CIOs FEATURED

DR. VAMSI MOHAN
Executive Director,
Pro-Code Platform Engineering,
code-wizard.ai

BHABANI CHATTERJEE
The Engagement Leader,
Capgemini

SATADAL BASU
Vice President Head IT Planning
and Development, AEON Credit Service
India Private Limited

GOKULAVAN JAYARAMAN
DGM - Compliance & Deputy CISO,
Lumina Datamatics Limited

AMIT GAUR
Senior Manager - IT,
Netcracker Technologies Solutions
India

INDEX

AI IN CYBERSECURITY, FRIEND OR FOE? A CXO'S GUIDE TO RESPONSIBLE IMPLEMENTATION

WHILE EMBRACING THE POTENTIAL OF AI TO ENHANCE SECURITY POSTURE, IT'S CRUCIAL TO UNDERSTAND AND MITIGATE ASSOCIATED RISKS.

By **Dr. Vamsi Mohan**

Cybersecurity threats are becoming increasingly sophisticated in today's rapidly evolving digital landscape. As organizations strive to protect their critical data and infrastructure, Artificial Intelligence (AI) has emerged as a powerful tool with the potential to revolutionize the cybersecurity landscape. However, AI also raises concerns surrounding potential misuse and unintended consequences. This begs the question: Is AI a friend or foe in cybersecurity?

For CXOs, navigating this complex terrain requires a balanced approach. While embracing the potential of AI to enhance security posture, it's crucial to understand and mitigate associated risks. This article explores the dual nature of AI in cybersecurity, offering insights and best practices for responsible implementation:

AI AS A FRIEND- BOOSTING SECURITY DEFENSES

AI offers several advantages in the fight against cybercrime:

- **Enhanced threat detection:** AI algorithms can analyze vast amounts of data in real-time, identifying anomalies and suspicious patterns that might escape human analysts. This allows for proactive detection of potential cyberattacks, enabling organizations to respond swiftly and mitigate risks.
- **Improved Security Automation:** AI can automate repetitive and time-consuming tasks like security log analysis and vulnerability scanning, freeing up human resources to focus on strategic initiatives and complex investigations.
- **Predictive Analytics:** AI can predict potential attacks by analyzing historical data and identifying patterns associated with past security breaches. This enables organizations to prioritize resources and take preventative measures to bolster their defenses against specific threats.

AI AS A POTENTIAL FOE- ADDRESSING RISKS AND CHALLENGES

While promising, AI implementation in cybersecurity also presents certain challenges:

- **Bias and explainability:** AI algorithms can inherit biases from the data they are trained on, potentially leading to discriminatory or inaccurate decisions. It's crucial to ensure unbiased training data and implement explainable AI models to understand how algorithms arrive at their conclusions.
- **Security vulnerabilities:** AI systems themselves can become targets for cyberattacks. Hackers could exploit vulnerabilities in AI models or manipulate training data to compromise security measures. Robust security protocols and continuous monitoring are essential to mitigate these risks.
- **Ethical considerations:** The use of AI in cybersecurity raises ethical concerns about privacy, transparency, and accountability. Organizations must establish clear ethical guidelines and ensure responsible AI development and deployment aligning with legal frameworks and societal values.

In this context, I'd like to share a case study of a Global Logistics Firm (GLF, actual customer name changed).

Challenge: GLF recently faced a sophisticated ransomware attack that encrypted critical data, disrupting operations and causing significant financial loss. Traditional security measures failed to detect the attack in its early stages.

AI solution:

- GLF implemented an AI-powered threat detection system that analyzes network traffic for anomalies.
- The AI identified unusual data transfer patterns associated with the ransomware deployment, triggering an immediate alert.
- Security teams quickly isolated the affected systems and contained the attack, minimizing data loss and downtime.

Benefits:

- AI's real-time analysis helped detect the attack significantly faster than manual methods.
- Early detection minimized the impact of the attack and expedited recovery efforts.
- The successful mitigation bolstered confidence in AI as a valuable security tool within GLF.

Implementation challenges:

- Integrating the AI system required initial investments in technology and training.
- Ensuring the AI model's accuracy and avoiding potential biases in its detection algorithms is crucial.

This case demonstrates the potential of AI to enhance security posture by proactively detecting and mitigating advanced threats. GLF is exploring further AI applications, such as automating security tasks and improving incident response processes.

This real-time case study highlights AI's potential as a “friend” in cybersecurity by showcasing its effectiveness in mitigating a real-world ransomware attack. It also acknowledges the ongoing challenges and emphasizes the importance of responsible AI implementation to maximize its benefits and minimize potential risks.

A CXO'S GUIDE TO RESPONSIBLE AI IMPLEMENTATION IN CYBERSECURITY

As CXOs, navigating the potential of AI while mitigating risks requires a proactive and responsible approach:

Educate employees about potential risks associated with AI and their role in upholding responsible use practices.

- **Clearly define objectives:** Define the specific security challenges you aim to address through AI. This ensures focused implementation and avoids the temptation to adopt AI for the sake of novelty.
- **Invest in explainable AI:** Choose and implement AI models that offer transparency and explainability in their decision-making processes. This allows for human oversight and ensures alignment with ethical guidelines.
- **Prioritize data security:** Implement robust data security practices to protect training data and AI models from unauthorized access or manipulation. Regularly audit and monitor data quality to prevent bias and ensure accurate results.
- **Build a culture of security awareness:** Foster a culture of security awareness within your organization. Educate employees about potential risks associated with AI and their role in upholding responsible use practices.
- **Collaborate with experts:** Partner with cybersecurity experts with the necessary skills and experience to guide AI implementation and address potential security vulnerabilities.

CONCLUSION

AI is a powerful tool with immense potential to transform the cybersecurity landscape. However, responsible implementation requires careful consideration of both benefits and risks. By adopting a balanced and proactive approach, CXOs can leverage the power of AI to enhance their security posture while mitigating potential pitfalls and upholding ethical considerations. Remember, AI in cybersecurity is not a silver bullet solution but a powerful tool that requires careful handling and integration within a comprehensive security strategy. ■

Dr. Vamsi Mohan is the Executive Director, Pro-Code Platform Engineering, code-wizard.ai

EMPOWERING CYBERSECURITY WITH CUTTING-EDGE GENERATIVE AI TECHNIQUES

BY HARNESSING THE POWER OF GEN AI, ORGANIZATIONS CAN STRENGTHEN THEIR CYBERSECURITY DEFENSES AND EFFECTIVELY SAFEGUARD AGAINST EVOLVING CYBER THREATS.

By **Bhabani Chatterjee**

Amidst the escalating tide of cyber threats, traditional cybersecurity methods dependent on rule-based systems and signature-based detection are increasingly falling short. Enter GenAI, a groundbreaking solution that harnesses the power of generative AI technologies such as generative adversarial networks (GANs), deep learning, and reinforcement learning, heralding a new era in cybersecurity defense trategies.

By autonomously assimilating extensive datasets and crafting innovative responses, GenAI emerges as a proactive force in identifying and thwarting cyber threats before they can wreak havoc. This paradigm shift promises to revolutionize the cybersecurity landscape, offering a dynamic and adaptive approach to safeguarding digital assets against evolving threats.

PRINCIPLES OF GENAI IN CYBERSECURITY

i. **Generative Adversarial Networks (GANs):** GANs, comprising a generator and a discriminator network, engage in a competitive learning process. In cybersecurity, GANs augment limited training datasets by generating realistic synthetic data, thereby enhancing anomaly detection systems' robustness.

ii. **Deep Learning:** Techniques like convolutional neural networks (CNNs) and recurrent neural networks (RNNs) empower GenAI systems to extract intricate patterns from extensive data, enabling advanced threat detection and classification.

iii. **Reinforcement Learning:** Reinforcement learning empowers GenAI agents to learn optimal decision-making strategies in dynamic environments. In cybersecurity, this enables adaptive responses to evolving threats, fortifying system resilience.

Methodologies and Applications of GenAI in Cybersecurity:

- **Threat Detection and Prevention:** GenAI analyzes network traffic, system logs, and user behavior to identify anomalies indicative of cyber threats, using unsupervised learning to detect previously unknown threats.
- **Vulnerability Assessment and Patch Management:** GenAI-powered vulnerability scanners prioritize vulnerabilities based on severity and exploitability, guiding effective patch management.
- **Threat Hunting and Incident Response:** GenAI algorithms proactively hunt threats by correlating security events, orchestrating timely responses to mitigate cyberattacks swiftly.

GENAI IN CYBERSECURITY BENEFITS

Generative AI (Gen AI) holds immense promise in transforming cybersecurity practices, offering a plethora of benefits that enhance defense mechanisms against evolving cyber threats:

a. Enhanced Threat Detection

Gen AI enables cybersecurity professionals to detect and understand cybersecurity threats more effectively by continuously analyzing vast datasets. Its ability to identify subtle behavioral variations indicative of potential attacks makes it particularly adept at pinpointing threats that traditional systems may overlook. By correlating user behavior and scrutinizing new files and code for suspicious activity, Gen AI enhances threat detection capabilities.

b. Predictive Analytics

Organizations can leverage Gen AI to make precise predictions of future cyber threats by analyzing repetitive patterns in extensive datasets such as security logs and network traffic. By extrapolating patterns from past vulnerabilities or attacks, Gen AI empowers proactive measures to mitigate potential threats effectively. This predictive capability enables organizations to stay one step ahead of cybercriminals and prevent security breaches before they occur.

c. Automated Responses

Gen AI automates responses to different types of cyber threats based on previously observed patterns and attacks. It can trigger actions such as blocking malicious IP addresses, adjusting firewall rules, or containing the spread of malware in real-time. Moreover, Gen AI can automate responses for patching security vulnerabilities preemptively or redirecting suspicious traffic for further investigation, streamlining incident response processes and reducing response times.

d. Deeper Insights into Vulnerabilities

By efficiently analyzing vast datasets, Gen AI provides deeper insights into vulnerabilities, enabling organizations to understand and address security weaknesses more effectively. Its ability to identify intricate patterns that may evade human analysts enhances vulnerability management practices, enabling organizations to proactively strengthen their security posture.

e. Proactive Risk Mitigation

Gen AI enables organizations to take a proactive approach to cybersecurity by identifying and addressing security vulnerabilities before they can be exploited by cybercriminals. Its predictive analytics capabilities empower organizations to anticipate and mitigate potential threats, minimizing the likelihood and impact of security breaches.

> **Just as generative AI can be used for defense, it can also be leveraged by attackers to create more sophisticated and evasive malware.**

f. Synergy with Human Expertise

While Gen AI offers significant advantages in fortifying cybersecurity measures, human intervention remains indispensable. A synergistic approach that leverages the strengths of both Gen AI and human expertise yields optimal results. Human analysts can validate predictions made by Gen AI, ensuring greater accuracy, while Gen AI can complement human expertise by automating routine tasks and providing valuable insights into emerging cyber threats.

In summary, Gen AI revolutionizes cybersecurity practices by enhancing threat detection, enabling predictive analytics, automating responses, providing deeper insights into vulnerabilities, enabling proactive risk mitigation, and synergizing with human expertise. By harnessing the power of Gen AI, organizations can strengthen their cybersecurity defenses and effectively safeguard against evolving cyber threats.

GENERATIVE AI VS TRADITIONAL CYBERSECURITY METHODS

Generative AI and traditional cybersecurity methods represent two different approaches to addressing security challenges, each with its own strengths and limitations. Here's a comparison of the two:

a. Generative AI:

- **Adaptability:** Generative AI, particularly in the context of cybersecurity, can adapt to new threats and attack vectors more rapidly than traditional methods. This is because generative AI systems can be trained on large datasets of both normal and malicious behavior, allowing them to detect anomalies and new attack patterns.
- **Automated Response:** Generative AI can automate certain aspects of cybersecurity, such as threat detection, incident response, and even patching vulnerabilities. This can help reduce the workload on human security teams and improve response times.
- **Potential for Evasion:** Just as generative AI can be used for defense, it can also be leveraged by attackers to create more sophisticated and evasive malware. This cat-and-mouse game can escalate as both sides continually adapt their tactics.
- **Data Requirements:** Generative AI models require large amounts of high-quality data to rain effectively. Obtaining and labeling such data can be challenging, especially when dealing with sensitive cybersecurity-related information.

b. Traditional Cybersecurity Methods:

- **Established Techniques:** Traditional cybersecurity methods rely on established techniques such as firewalls, intrusion detection systems, antivirus software, and access controls. These methods have been refined over time and are well-understood by security professionals.
- **Human Expertise:** Traditional cybersecurity methods often rely heavily on human expertise for threat analysis, incident response, and decision-making. Experienced

cybersecurity professionals can provide valuable insights and judgment that may not be easily replicated by AI.

- **Limited Scalability:** Traditional cybersecurity methods may struggle to scale effectively, particularly in the face of rapidly evolving threats and a growing attack surface. Human analysts can only handle so much data and may miss subtle indicators of compromise.
- **Rule-Based:** Many traditional cybersecurity methods are rule-based, meaning they rely on predefined signatures or heuristics to detect threats. While effective against known threats, these methods may struggle with detecting novel or sophisticated attacks.

In summary, generative AI offers the potential for more adaptive and automated cybersecurity solutions, while traditional methods provide a foundation of established techniques and human expertise. A holistic approach to cybersecurity often involves leveraging the strengths of both approaches to provide robust protection against a wide range of threats.

A holistic approach to cybersecurity often involves leveraging the strengths of both approaches to provide robust protection against a wide range of threats.

REAL-WORLD APPLICATIONS AND CASE STUDIES OF GEN AI IN CYBERSECURITY

In the realm of cybersecurity, real-world examples vividly illustrate the transformative impact of integrating generative AI and Artificial Intelligence (AI) technologies to fortify defenses against evolving cyber threats. Across industries, AI applications are increasingly recognized as crucial tools for enhancing security measures, bolstering threat detection capabilities, and fortifying digital infrastructures. Let's explore some compelling instances to grasp how AI can effectively mitigate cyber risks.

Acknowledging the vast potential of generative AI, particularly in mitigating the severe shortage of skilled professionals in the cybersecurity industry, Capgemini recognizes four critical perspectives that provide a comprehensive understanding of GenAI's role in the future of cybersecurity:

a. **Efficiency:** Generative AI has the potential to enhance efficiency in cybersecurity through automation and algorithmic optimization, allowing human experts to concentrate on strategic challenges.

b. **Enhanced Security Effectiveness:** By leveraging AI capabilities, organizations can bolster their threat detection and response efforts, staying ahead of evolving cyber threats.

c. **End-to-End Security:** Generative AI ensures comprehensive security by integrating advanced access control mechanisms and preserving data integrity, fostering trust in cybersecurity practices.

d. **Defense Against AI-Generated Fraud:** Generative AI acts as a defense against AI-generated fraud, identifying and mitigating threats to safeguard digital landscapes from evolving risks.

Capgemini has harnessed the power of GenAI for Threat Detection and implemented Defensive mechanisms in various areas:

i. **Autonomous Threat Detection:** A financial institution reduced false positives in phishing attack detection by using Generative Adversarial Networks (GANs) to train its intrusion detection system.

ii. **Adaptive Defense:** A multinational corporation improved its security posture by dynamically adjusting access controls based on reinforcement learning.

iii. **Threat Intelligence Fusion:** A government agency preemptively countered nation-state cyber espionage campaigns by leveraging deep learning-based threat intelligence.

Through these initiatives, Capgemini demonstrates the practical application of Generative AI in cybersecurity, showcasing its potential to address key challenges and enhance security measures effectively.

Some more real-world examples:

- Beyond safeguarding its own digital ecosystem, Google is actively leveraging generative AI to develop innovative solutions aimed at enhancing cybersecurity across organizations. Notably, Google has introduced initiatives such as the Secure AI Framework (SAIF) as part of its commitment to bolstering cybersecurity standards. SAIF serves as a conceptual framework designed to safeguard AI systems against a myriad of threats and attacks. It addresses risks ranging from potential theft of AI models to data poisoning through generative AI outputs and malicious input injections. SAIF is instrumental in monitoring inputs and outputs to detect and counteract threats by automating defense mechanisms effectively. Additionally, Google is poised to unveil Magika, a cybersecurity tool engineered to identify file types and detect malware. Successfully deployed within Google's ecosystem to safeguard products like Google Drive, Gmail, and Safe Browsing, Magika exemplifies Google's proactive stance in combatting cyber threats.

- As a globally recognized payment platform facilitating seamless transactions for merchants and consumers alike, PayPal relies on advanced Machine Learning (ML) models to bolster cybersecurity measures. Leveraging its extensive network, PayPal harnesses AI capabilities to detect fraudulent activities in real-time. The platform's vast repository of transaction data serves as a rich source for AI algorithms to continuously learn and refine their detection mechanisms. The insights gleaned from these ML models not only enhance authentication systems but also enable PayPal to swiftly identify and mitigate fraudulent transactions. As PayPal's dataset expands, the ML models continue to evolve and adapt, exemplifying the dynamic nature of AI driven cybersecurity measures.

In summary, these real-world examples underscore the pivotal role of AI, particularly generative AI, in fortifying cybersecurity defenses and safeguarding digital assets against a constantly evolving threat landscape. Through strategic integration of AI technologies, organizations like Google and PayPal are at the forefront of innovation, proactively mitigating cyber risks and bolstering resilience in an increasingly digital world.

Emerging Trends in AI and Cybersecurity:

Generative AI is rapidly evolving within the cybersecurity landscape, paving the way for several emerging trends that are poised to shape the future of digital defense.

a. Integration of AI with Cloud Security:

The convergence of AI systems with cloud infrastructure is gaining momentum, facilitating real-time threat detection and prevention. This integration promises to bolster cybersecurity by leveraging AI's analytical capabilities in conjunction with the scalability and agility offered by cloud platforms.

b. Expansion of Gen AI-powered Tools:

Gen AI is proving to be invaluable in the creation of deceptive systems, such as fake environments or honeypots, to mislead cyber attackers. Additionally, its proficiency in analyzing vast datasets and identifying patterns is driving the development of novel cybersecurity solutions tailored to combat evolving threats.

c. Emphasis on Cyber Resilience:

AI's predictive capabilities are enhancing the resilience of cybersecurity systems by enabling proactive identification and patching of vulnerabilities before they can be exploited by attackers. This proactive approach to threat mitigation is instrumental in fortifying digital infrastructures against emerging cyber threats.

d. Sophistication of Cyber-Attacks Facilitated by Gen AI:

The proliferation of Gen AI is empowering cyber attackers to orchestrate sophisticated and large-scale cyberattacks with greater efficiency. Deep fakes, fueled by advancements in generative AI, pose an elevated risk of social engineering through personalized phishing campaigns, highlighting the need for robust cybersecurity measures.

e. AI-Powered Automation Enabling Enhanced Insights:

AI-driven automation is revolutionizing cybersecurity operations by streamlining time-consuming tasks such as log review, threat detection, and analysis. This automation liberates human experts to focus on strategic endeavors like decision-making and developing comprehensive cybersecurity strategies, fostering a symbiotic relationship between human expertise and AI systems.

f. Rise in Specialized Language Models:

While large language models have demonstrated efficacy in processing vast datasets, specialized domains like cybersecurity necessitate more precise and actionable insights. Consequently, there is a growing trend towards the adoption of smaller and specialized language models tailored to address the unique challenges of cybersecurity operations.

g. Focus on Proactive Threat Detection in Mobile Applications:

Gen AI is increasingly being deployed to enhance the security of mobile applications by prioritizing proactive threat detection and real time responses. By analyzing user behavior, AI can detect anomalies indicative of security breaches, such as unusual login attempts or suspicious activity, thereby bolstering the resilience of mobile app ecosystems against cyber threats.

As we gaze into the future of AI in cybersecurity, it is evident that continued innovation will yield more advanced tools and platforms to combat the ever-evolving threat landscape, underscoring the critical importance of proactive defense strategies in safeguarding digital assets and infrastructure.

ETHICAL AND REGULATORY CONSIDERATIONS

The increasing utilization of Generative AI underscores the necessity for regulatory frameworks to ensure ethical adoption and transparent risk management. Ideally, the deployment of AI tools should adhere to the guidelines established by existing regulatory bodies, with laws such as the GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act) setting stringent standards for user privacy and data protection within AI cybersecurity models. These regulations typically include:

i. Collecting and using only necessary data for specific and legitimate purposes.

ii. Implementing robust measures to safeguard user data from unauthorized access or misuse.

iii. Providing clear and comprehensive information to users regarding the functioning of AI platforms and how their data is utilized.

Moreover, established frameworks for ethical AI adoption emphasize principles such as fairness, transparency, accountability, and robustness.

In addition to regulatory compliance and ethical frameworks, the concept of Human-centered design advocates for the development of AI systems with a focus on human needs rather than purely technical considerations. This approach ensures that AI solutions are user-friendly, accessible, and aligned with societal values and expectations.

EXPERT OPINIONS AND FORECASTS ON USING GEN AI FOR CYBERSECURITY

Cybersecurity experts unanimously agree on the transformative potential of generative AI in revolutionizing cybersecurity practices, offering proactive defense measures against evolving cyber threats.

- **Kunle Fadeyi, a member of Forbes Technology Council,** stresses the profound impact of AI in bolstering cybersecurity. He advocates for a "security by design" approach, which involves identifying and rectifying security vulnerabilities before cybercriminals can exploit them. This proactive stance is crucial for safeguarding digital assets and mitigating the risks posed by cyberattacks.
- **Mike Lieberman, CTO of Kusari,** envisions AI playing a pivotal role in enhancing cybersecurity efforts by detecting malicious patterns within code or configurations. Lieberman emphasizes that AI should act as a guiding force in navigating complex security scenarios, providing valuable insights to cybersecurity professionals. However, he emphasizes the importance of using AI tools as signals rather than sole decision-makers, highlighting the need for human oversight in cybersecurity operations.

> **Cybersecurity experts unanimously agree on the transformative potential of generative AI in revolutionizing cybersecurity practices, offering proactive defense measures against evolving cyber threats.**

Together, these insights from cybersecurity experts underscore the pivotal role of generative AI in fortifying cybersecurity defenses, driving proactive risk mitigation, and ensuring the resilience of digital infrastructures against evolving cyber threats. By embracing AI-driven approaches and integrating cybersecurity into overarching business strategies, organizations can effectively safeguard against cyber risks and uphold the trust of stakeholders.

Challenges and Future Directions:

Despite its transformative potential, Generative AI (GenAI) in cybersecurity confronts several challenges, including concerns regarding data privacy, adversarial attacks, and algorithmic biases. Addressing these challenges requires interdisciplinary research efforts and collaboration among academia, industry, and policymakers. Future directions for GenAI in cybersecurity include the development of explainable AI techniques, federated learning approaches for collaborative threat intelligence sharing, and the integration of blockchain technology to enhance data integrity and trustworthiness.

Generative AI stands as a powerful force in cybersecurity, promising to revolutionize security practices while simultaneously enhancing the capabilities of malicious actors. As technological advancements accelerate, chief security officers (CSOs) must prepare for an ever-changing landscape.

In conclusion, GenAI represents a paradigm shift in cybersecurity, empowering organizations to proactively defend against evolving threats. As GenAI continues to evolve, its integration promises to revolutionize threat detection, incident response, and vulnerability management, ensuring a safer cyber landscape. ■

Mr. Bhabani Chatterjee is the Engagement Leader of Capgemini.

CYBERSECURITY GOVERNANCE: THE COLLABORATIVE APPROACH TO PROTECTING DIGITAL ASSETS

WITH THE GROWING COMPLEXITY AND SCALE OF CYBER THREATS, THE RESPONSIBILITY OF CYBERSECURITY GOVERNANCE HAS EXPANDED BEYOND THE IT DEPARTMENT. IT NOW INVOLVES A DIVERSE GROUP OF STAKEHOLDERS.

By **Satadal Basu**

"Thinking cybersecurity is not your job or believing cybersecurity is solely IT's responsibility" is like saying safety is not your concern while driving. We all play a crucial role in safeguarding our digital world and the protection of our digital assets and information."

In today's fast-paced digital landscape, cybersecurity has become a top priority for businesses across all industries. With the growing complexity and scale of cyber threats, the responsibility of cybersecurity governance has expanded beyond the IT department. It now involves a diverse group of stakeholders.

In this article, we will explore how the roles and responsibilities of various stakeholders in cybersecurity governance have evolved and how they collaborate to ensure the protection of digital assets and data.

EXECUTIVE LEADERSHIP:

Leadership at the executive level plays a crucial role in cybersecurity governance. Top-level executives, including CEOs, CIOs, and CISOs, have the responsibility to set the agenda and provide overall direction for cybersecurity initiatives within their organizations. They are tasked with allocating resources, fostering a strong understanding of cybersecurity, and ensuring that it is integrated into the company's overarching objectives. By demonstrating a strong commitment to cybersecurity, these executives can instill a culture of security throughout the entire organization.

IT DEPARTMENT:

The IT department is responsible for managing and implementing cybersecurity measures. This team of IT professionals is accountable for installing security technologies, monitoring potential threats in networks, and addressing security incidents. They maintain the security of the organization's infrastructure, applications, and data. Besides possessing technical skills, IT professionals should also have effective communication skills to work with other stakeholders and explain complex security concepts to non-technical individuals.

RISK MANAGEMENT AND COMPLIANCE TEAMS:

Risk management and compliance teams are tasked with a number of important responsibilities that are critical to ensuring the safety and security of an organization's digital infrastructure. At the heart of their duties lies the need to evaluate an organization's cybersecurity risks and identify potential vulnerabilities. This involves a thorough examination of the organization's digital assets, including networks, servers, databases, applications, and other key resources.

Once potential risks have been identified, risk management and compliance teams collaborate closely with IT and top management to develop risk-reduction tactics and establish protective measures against cyber dangers. This might involve implementing advanced security protocols, upgrading software and hardware, or creating new policies and procedures to ensure compliance with industry regulations and standards.

To stay on top of potential cybersecurity threats, risk management and compliance teams conduct frequent

Risk management and compliance teams are tasked with a number of important responsibilities that are critical to ensuring the safety and security of an organization's digital infrastructure.

risk evaluations and keep up to date with emerging trends and best practices. By staying informed and vigilant, these teams can help organizations anticipate and resolve potential security vulnerabilities before they can be exploited by malicious actors.

Overall, the work of risk management and compliance teams is essential to ensuring the continued safety and security of an organization's digital infrastructure. Through their expertise and diligence, they help organizations stay protected against cyber threats and maintain the trust and confidence of their stakeholders.

HUMAN RESOURCES:

The participation of human resources departments in cybersecurity governance is on the rise, with a focus on employee training and awareness. HR experts have a crucial responsibility in educating staff on effective cybersecurity methods, enforcing security protocols, and performing background checks to minimize the risk of insider threats. By cultivating a security-oriented environment and encouraging employee responsibility, HR departments contribute significantly to the organization's ability to withstand cyber-attacks.

LEGAL AND COMPLIANCE DEPARTMENTS:

The legal and compliance departments have the responsibility of ensuring that the cybersecurity practices of the organization comply with all regulatory and legal obligations. They are tasked with navigating the complex data privacy laws, developing cybersecurity policies and procedures, and representing the organization in any legal cases relating to cybersecurity breaches. By providing legal counsel and ensuring compliance with relevant regulations, these departments play a critical role in reducing the legal and reputational risks that arise from cybersecurity incidents.

MARKETING AND SALES DEPARTMENTS:

The efficient handling of cybersecurity requires the active involvement of marketing and sales teams in promoting cybersecurity awareness among clients and customers. These teams are accountable for communicating the company's commitment to security and educating customers on how to practice safe online practices. Through different initiatives, such as marketing campaigns and ensuring that security is addressed in client interactions and contracts, marketing and sales teams can establish trust and improve the organization's reputation in the market.

THIRD-PARTY VENDORS AND PARTNERS:

Third-party vendors and partners can pose a significant cybersecurity threat to organizations. To minimize this risk, organizations should build strong partnerships with vendors by ensuring their compliance with security standards, implementation of necessary safeguards, and frequent security evaluations. By including strict security requirements in vendor contracts and conducting thorough due diligence on third-party vendors, organizations can effectively reduce the potential for supply chain attacks and data breaches.

EMPLOYEES:

Organizations often view employees as the weakest link in cybersecurity governance. However, employees play a crucial role in managing cyber risks. To ensure the security of the organization, it is important to create a culture of cybersecurity awareness among employees. This can be achieved by providing continuous training, promoting good security practices, and encouraging employees to report any suspicious activities. By empowering employees to take an active role in cybersecurity governance, organizations can effectively reduce the chances of insider threats and human error leading to security breaches.

CONCLUSION:

Effective management of cybersecurity requires collaboration among various parties in an organization. This includes top-level executives, IT specialists, risk management personnel, human resources, marketing and sales teams, and all employees. Each stakeholder has a vital role to play in defending against cyber threats. By acknowledging the constantly evolving nature of cyber risks and adopting a comprehensive approach to governance, companies can strengthen their cybersecurity defenses and minimize the impact of cyber-attacks in today's digital landscape. By working together, these stakeholders form a united front against cyber threats, cooperating to safeguard sensitive information, maintain customer confidence, and protect the integrity of the organization's digital infrastructure. Through shared dedication to implementing cybersecurity best practices and ongoing cooperation, companies can confidently navigate the complexities of the digital age with strength and resilience. ■

Satadal Basu is the Vice President - Head IT Planning and Development at AEON Credit Service India Private Limited

CYBER SECURITY OWNERSHIP: WHO IS RESPONSIBLE?

RESPONSIBILITIES BETWEEN CISOS AND CIOS IN ENSURING A ROBUST CYBERSECURITY POSTURE WITHIN ORGANIZATIONS

By **Gokulavan Jayaraman**

COLLABORATIVE CYBERSECURITY RESPONSIBILITY

A vanilla answer would be "it's everyone's responsibility," however the topic here is how there can be a collaborative approach and shared responsibility between CISO & CIO for organizational cybersecurity wellbeing.

Most of the, the organizations' structure, hierarchy and culture are not always that simple to give the CISOs or CIOs the complete power to work on their core strength and knowledge. This is where the thin line builds into a crack or sometimes a gap.

CISOs & CIOs are generally well equipped to do the risk analysis related to cybersecurity and apply necessary treatments that are more appropriate to the organization. They play an important role in writing policies, procedures, implementation, compliance and regular monitoring through SOC and other vital feeds to ensure organizational security posture is of highest standard. A perfect approach would be on playing with the strength of the CISO & CIO on the above aspects and share the responsibility mutually.

UNDERSTANDING CISO VS CIO

Chief Information Security Officer (CISO): The CISO is typically responsible for an organization's information and data security. This role is mainly responsible for creating and implementing the organization's security strategy, managing security with tech, people & partners, and responding to security incidents. The CISOs primary aim is to protect the organization from internal and external security threats therefore ensuring compliance with regulatory requirements related to information security.

Chief Information Officer (CIO): The CIO is generally responsible for the complete information technology (IT) strategy and the implementation of technology within the organization. While their primary focus is on leveraging technology to support the business's goals and objectives, they

also play a role in ensuring the security of the IT infrastructure and Secure Development or DevSecOps. In some organizations, especially the smaller in nature, the CIO may directly oversee cybersecurity efforts if there is no CISO.

The CISOs role is expanding to encompass broader security threats within the industry landscape.

THE FUTURE OF TAKING SHARED RESPONSIBILITIES.

Developing a strong data security and privacy protection strategy throughout an organization is crucial. To achieve this, it's vital for the CISO and the CIO to collaborate closely. This collaboration ensures that the organization not only meets compliance standards but also maintains exceptional security hygiene.

In the past, a clear division existed between the CISO, who oversaw organizational security, and the CIO, who focused on technical innovation and implementation.

However, a shift is occurring. The CISOs role is expanding to encompass broader security threats within the industry landscape, while the CIO continues to manage the tactical execution of security initiatives. This collaboration fosters a more integrated approach to security, strengthening overall effectiveness. It is important to acknowledge that the specific responsibilities of both roles can vary depending on the organization. For instance, some CISOs might actively participate in frontline cyber defense, while others provide strategic oversight. The size and industry of the organization can also influence the scope of the CISO's duties, with some handling both strategic and tactical responsibilities.

Both the CISO and CIO face increased pressure to detect and resolve cyber threats while promoting robust security practices. This necessitates tight collaboration and alignment between these roles. To effectively secure all endpoints, they should prioritize fostering a culture of continuous innovation and resilience across all aspects of their work.

Notably, the CIO remains responsible for managing the organization's technological infrastructure, ensuring seamless operations while the CISO prioritizes protecting that infrastructure from cyber threats.

Though traditionally distinct in focus, the CISO and CIO roles are intricately linked, playing crucial parts in safeguarding the organization from any adversity and make the organization sail smoothly towards it's context/objective. A strong connection thrives on mutual dependence, and this starts with prioritizing critical business outcomes over individual preferences. Achieving a sustainable balance necessitates continuous exploration of collaborative opportunities, which plays on the strength of the CISO and CIO.

Harmonizing the CISO and CIO roles is crucial to the organizations security culture, if we take care of the following points in the relationship:

- CISO & CIO should treat each other as peers
- Establish a clear understanding of responsibilties.
- Know the strength of each other and play with the strength.
- Should involve together in organization's strategic planning.
- Should continously upskill themselves
- Importantly have a healthy positive relationship. ■

Gokulavan Jayaraman is the DGM - Compliance & Deputy CISO, Lumina Datamatics Limited

BATTLING IT STAFFING SHORTAGES

THE RISE IN SOPHISTICATED CYBER THREATS HAS LED TO A SIGNIFICANT INCREASE IN DEMAND FOR SKILLED CYBERSECURITY PROFESSIONALS.

By **Amit Gaur**

In today's rapidly digitizing world, cybersecurity is a key concern for both businesses and government agencies. As cyber threats become more sophisticated and prevalent, the demand for skilled cybersecurity professionals has increased significantly, resulting in a critical IT and cybersecurity talent shortage."

This article addresses the causes of these workforce challenges and comprehensively examines effective strategies and best practices aimed at attracting and retaining top cybersecurity talent.

ADDRESSING THE SKILLS SHORTAGE

The cybersecurity skills shortage is a complex problem caused by a combination of rapid technological innovation, increasing cyber threats, and a lack of educational programs that meet the changing needs of the industry.

The imbalance between the pool of available skilled talent and the growing demand for that expertise will further expose organizations to cyber risks.

This problem is further exacerbated by the high turnover rate in the IT industry.

In the IT industry, professionals frequently change roles in search of better prospects and new challenges.

INNOVATIVE RECRUITMENT STRATEGIES FOR CYBERSECURITY TALENT

1. **Build educational partnerships:** Closing the talent gap requires building strong partnerships with academic institutions. These collaborations create internship and training opportunities that provide students with hands-on experience and a seamless entry into the cybersecurity field.
2. **Prioritize upskilling and reskilling efforts:** Companies can leverage their existing workforce to alleviate talent shortages by implementing comprehensive upskilling and reskilling efforts. Businesses can accelerate the cybersecurity skills of their current workforce by accessing a variety of online learning modules, certification programs, and hands-on training workshops.
3. **Refreshing recruitment tactics:** Introducing innovative recruitment strategies. Using specialized job boards, leveraging social media platforms, and working with recruitment agencies that specialize in technology roles can help you discover hidden talent. Additionally, emphasizing the impactful and mission-oriented aspects of cybersecurity roles can attract individuals driven by a desire to make a big impact.
4. **Promoting Diversity and Inclusion:** Expanding the talent pool through diverse and inclusive hiring practices can significantly reduce talent shortages. Encouraging diversity not only fosters innovation and improves problem-solving

The imbalance between the pool of available skilled talent and the growing demand for that expertise will further expose organizations to cyber risks.

Emphasizing the impactful and mission-oriented aspects of cybersecurity roles can attract individuals driven by a desire to make a big impact.

skills, it taps previously underutilized parts of the workforce and strengthens the pool of potential cybersecurity candidates.

STRATEGIES FOR RETAINING CYBERSECURITY TALENT

1. **Offer Competitive Compensation:** To ensure the retention of top talent, companies can offer competitive compensation, bonuses, and inclusions that meet the unique requirements of the cybersecurity field. It is essential to offer an attractive compensation package with comprehensive benefits and other incentives.
2. **Fostering career advancement:** To keep cybersecurity professionals engaged and motivated, it's important to provide clear career paths and opportunities for continuous professional development.
3. **Building a Positive Work Environment:** A work culture that promotes inclusivity, values innovation, and recognizes individual achievement plays a critical role in retaining qualified professionals.
4. **Leveraging Flexibility:** In today's labor market, the ability to offer flexible working conditions, including remote work options, is increasingly important for employee retention.

EMPHASIS ON TECHNOLOGY AND AUTOMATION:

The strategic use of automation tools and the integration of artificial intelligence into cybersecurity operations reduces the workload of cybersecurity teams, allowing them to spend more time on strategic needs.

Additionally, the introduction of these cutting-edge technologies can be an attractive prospect for potential employees looking to stay at the forefront of cybersecurity advances.

FINAL THOUGHTS:

Addressing the cybersecurity skills shortage requires a comprehensive strategy that includes both acquiring new talent and retaining existing professionals.

By building educational partnerships, fostering upskilling and reskilling efforts, embracing technological innovation, and fostering inclusive and collaborative workplace cultures, companies can effectively address the challenges posed by the talent gap.

As the cyber threat landscape continues to evolve, so must our approaches to developing and maintaining cybersecurity professionals equipped to protect against these threats. ■

Amit Gaur is the Senior Manager - IT, Netcracker Technologies Solutions India

The Algorithmic You: How AI Shapes Your Reality

By 2030, AI's impact is projected to contribute $15.7 trillion to the global economy, a harmonious combination of $6.6 trillion in productivity gains and $9.1 trillion in the rhythmic progression of consumption.

By **Iccha Sharma**

The world is changing at AI's pace, with people dancing to a new tune.

Remember the days when "artificial intelligence" belonged solely to science? Those days are gone. AI, once a futuristic fantasy, has crept into every corner of our lives, silently orchestrating our routines from waking up to the minute we drift off to sleep.

AI algorithms power our digital companions, smartphones, voice assistants, and smartwatches, whispering suggestions, anticipating needs, and learning our preferences with uncanny accuracy. But amidst the undeniable convenience, a question lingers: are we puppets in this grand algorithmic play, or are we active participants in shaping our AI-infused reality? As AI becomes an integral part of our lives, its economic impact is noteworthy. The global market is to transform into a dynamic scenario, moving to a substantial $267 billion by 2027, driven by a CAGR of 33.2%

Yuval Noah Harari, historian and author of "Sapiens: A Brief History of Humankind," echoes this sentiment, cautioning that "humans are hackable animals now," vulnerable to manipulation through meticulously crafted algorithms.

AI in our pockets- a double-edged sword

Over 5.3 billion people, nearly 70% of the global population, use smartphones today, generating and consuming 2 exabytes of data daily – enough to fill all the hard drives in the world 185 times over. This staggering volume is where AI truly shines. Algorithms tirelessly analyze our digital footprints, learning our quirks and routines with uncanny accuracy. They recommend restaurants tailored to our palates, translate spontaneous conversations with distant relatives, and even identify suspicious activity, protecting us from online threats.

By 2030, AI's impact is projected to contribute $15.7 trillion to the global economy, a harmonious combination of $6.6 trillion in productivity gains and $9.1 trillion in the rhythmic progression of consumption. Once considered a novelty, voice search is now adopted by 35% of companies, a trend set to expand as AI assistants become more proficient. Similarly, self-driving cars, resembling futuristic chariots, are poised to join the procession, with one in ten cars expected to be autonomous by 2030.

"We are becoming algorithmic selves," warns Sherry Turkle, a renowned psychologist, noting the erosion of real-world connections as we turn to AI for companionship and validation.

Hence, amidst the convenience, shadows lurk. Biases embedded in algorithms, often unintentional yet deeply impactful, can lead to discriminatory practices like unfair loan approvals and biased hiring decisions. Our insatiable reliance on these digital companions raises concerns about digital addiction and social isolation, leaving us yearning for genuine human connection in the glow of our screens.

AI-powered platforms tailor learning experiences to individual needs in education, catering to different learning styles and paces. Even mundane tasks like driving are redefined by AI, with self-driving cars promising efficiency and potentially saving millions of lives from traffic accidents.

The pervasive presence of AI

AI's reach extends far beyond our pockets, silently transforming nearly every facet of our lives. In healthcare, algorithms analyze medical scans with superhuman precision, detecting diseases early and paving the way for personalized treatment plans. AI-powered platforms tailor learning experiences to individual needs in education, catering to different learning styles and paces. Even mundane tasks like driving are redefined by AI, with self-driving cars promising efficiency and potentially saving millions of lives from traffic accidents. By 2025, AI-powered robots are expected to handle 52% of manufacturing tasks, a significant increase from their 10% involvement in 2015.

While our smartphones may be the most visible face of AI, its influence stretches far beyond our pockets, quietly weaving itself into the fabric of daily life. Imagine waking up to your smart thermostat setting the perfect temperature before you even throw off the covers, thanks to its AI brain anticipating your morning routine. As you brew your coffee, you chat with your friendly voice assistant, asking for the latest news and weather updates – a personalized briefing curated by algorithms learning your interests and location.

Throughout your day, AI guides you on unseen paths. Your GPS, no longer just a digital map, predicts traffic with uncanny accuracy, rerouting you through the maze of city streets to ensure a smooth commute. At work, AI filters your overflowing inbox, intelligently separating the critical from the mundane, and even suggests witty email replies, saving you precious time.

At lunchtime, you scroll through your social media feed, a carefully curated field by AI algorithms. They know your favorite coffee shop photos, your love for travel documentaries, and the friends you haven't spoken to in a while – each post a gentle nudge of reconnection. As you head to the gym, your fitness tracker, empowered by AI, analyzes your every step, offering personalized coaching and cheering you on to reach your goals.

Back home, your smart home awaits. AI anticipates your arrival, dimming the lights and activating the security system. Hungry? No need to scroll through endless recipes. Your fridge, stocked with groceries ordered through an AI-powered shopping app, suggests the perfect meal based on your dietary preferences and what's left on the shelves. As you curl up with a book, your AI-powered reading app recommends similar titles, tailoring your literary journey to your unique tastes.

And when it's time to sleep, your smart bedroom adjusts the temperature and plays calming music, all orchestrated by AI's invisible hand. This symphony of automation is not just about convenience; it's about understanding your needs, anticipating your desires, and freeing you to focus on what truly matters.

However, amidst this orchestrated reality, challenges remain. Social media algorithms can create echo chambers while serving up personalized content, reinforcing our biases and isolating us from opposing viewpoints. AI-powered customer service chatbots, while efficient, may lack the empathy and nuance of human interaction.

As Fei-Fei Li, director of Stanford's AI Laboratory, reminds us, "We need to ensure that AI technology enhances and complements human strengths, not replaces them."

Businesses find the benefits worth the engagement. 64% believe AI will enhance their productivity, a sentiment echoed by 76% who anticipate AI creating new roles rather than displacing existing ones. Nonetheless, concerns persist. Like murmurs in a crowded room, 75% of consumers worry about AI's potential for spreading misinformation, and 41% fear its impact on society.

As Elon Musk warns, "With artificial intelligence, we are summoning the demon." This necessitates responsible development, ensuring AI aligns with human values and serves as a tool for good, not an instrument of division or destruction.

The displacement of jobs by automation remains a pressing concern. While AI creates new opportunities, it also disrupts existing workflows, leaving some in the digital dust. The challenge lies in harnessing AI's potential for good while mitigating its negative consequences, ensuring a harmonious future where humans and machines coexist.

Future AI trends

The future beckons with even more profound integrations of AI into our lives. Imagine smart homes anticipating our needs, adjusting temperature and lighting before we even step through the door. Self-driving cars weave through cityscapes without human intervention, freeing up our time for creative pursuits or meaningful conversations. And perhaps, in the not-so-distant future, AI doctors will analyze our health data, predicting and preventing illnesses before they manifest.

The possibilities are both exhilarating and daunting. While AI promises enhanced convenience, improved health, and greater access to information, it also raises questions about job displacement, ethical dilemmas, and potential misuse.

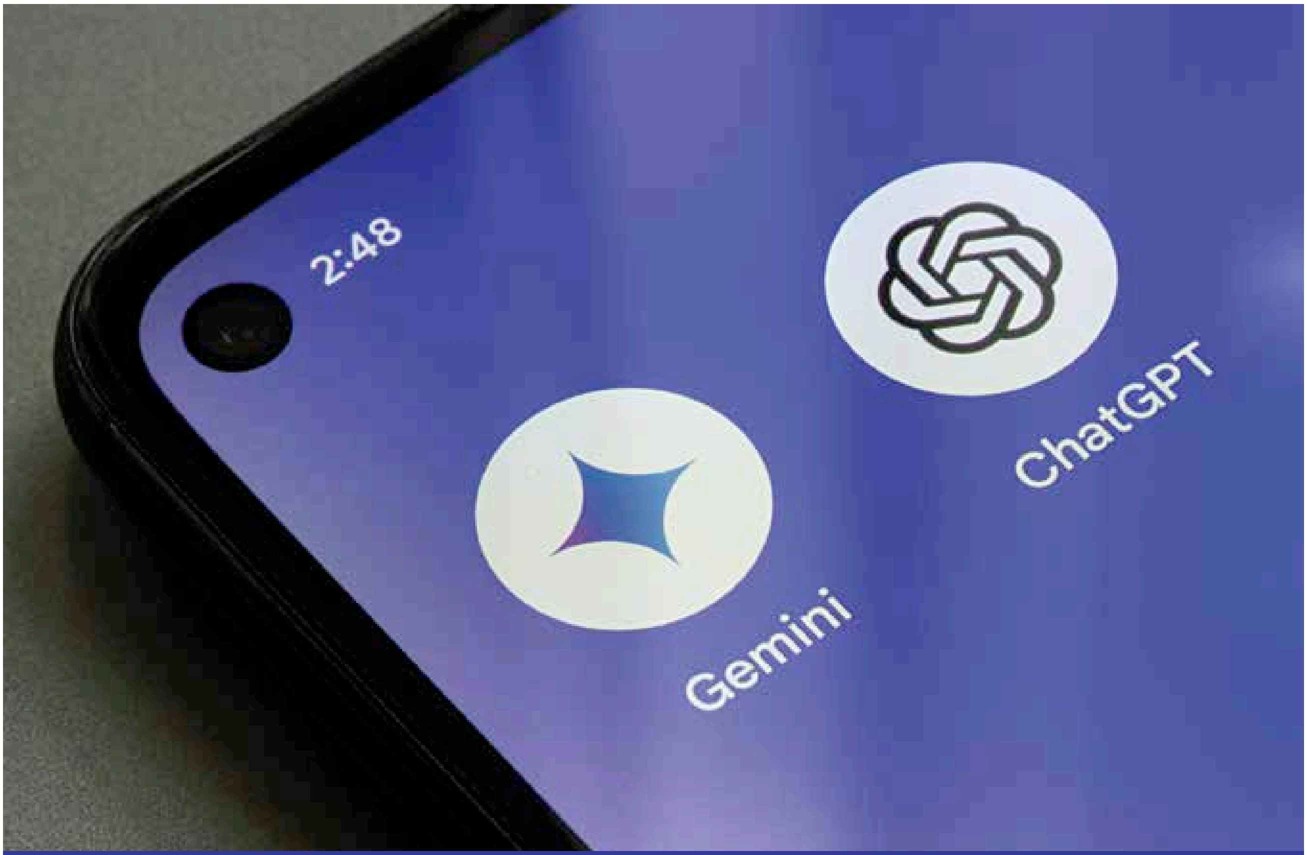
As Elon Musk warns, "With artificial intelligence, we are summoning the demon." This necessitates responsible development, ensuring AI aligns with human values and serves as a tool for good, not an instrument of division or destruction.

AI is not an external force invading our lives; it is the reflection of our ingenuity woven into the fabric of our everyday reality. We are not simply consumers of AI's offerings; we are the architects, shaping its development and directing its course. The question, then, is not whether AI will control us but how we will choose to control AI.

We can navigate this new frontier with purpose and prudence by understanding the intricate dance between AI and our daily lives, acknowledging its transformative potential, and recognizing its inherent anxieties. The future we create with AI depends not on algorithms and processors but on our choices today. So, let us choose wisely, ensuring that AI remains a tool that empowers us, not a puppeteer that controls us.

Ultimately, the dance between man and machine is a waltz in progress. We, the architects, hold the reins, shaping the future of AI with each choice we make. By understanding its transformative potential, acknowledging its inherent anxieties, and navigating this frontier with purpose and prudence, we can ensure that AI remains a partner in progress, not a puppet master dictating our reality. ■

Ichha Sharma is an Editor at Digit.



Will Google Gemini Outshine ChatGPT? Insights from CIOs

As AI continues evolving, LLMs present immense opportunities for businesses and individuals.

By **Nisha Sharma**

Generative AI tools are making a significant impact on how we interact and the outcomes we produce in record time. For enterprises, they hold immense potential to become a new genie, ready to transform numerous processes, aiding in accomplishing tasks and activities faster and more efficiently.

A report by Valuates Report disclosed that The Large Language Model (LLM) Market was valued at 10.5 Billion USD in 2022 and is anticipated to reach 40.8 Billion USD by 2029, witnessing a CAGR of 21.4% during the forecast period 2023-2029.

While Microsoft-backed OpenAI's ChatGPT currently holds an undisputed leadership position, Google is also preparing to leverage its extensive experience with data by testing and launching its family of multimodal large language models, the latest being Google Gemini.

While both platforms offer unique qualities poised to make a significant impact on AI development, the question remains: which one currently excites CIOs and enterprises more?

OpenAI ChatGPT- the conversational maestro

OpenAI's ChatGPT has been a disruptor since its inception, renowned for its ability to generate natural language responses that are remarkably human-like. ChatGPT generates coherent and contextually relevant text using a sophisticated neural network architecture based on vast datasets. Its applications span various domains, including customer service, content creation, and education, showcasing its versatility and adaptability.

Deepak Agarwal, Ex-Executive Director, Indian Oil Corporation, notes, "ChatGPT's natural language processing capabilities enable it to generate responses that can significantly enhance user interaction and satisfaction." However, he also cautions against its limitations, such as potential biases and a fixed knowledge base, which necessitate careful curation of training data and ongoing model refinements.

Google Gemini AI- the multimodal innovator

In contrast, Google's Gemini AI represents the cutting edge of multimodal AI technology. Gemini AI embodies the future of AI's multimodal interaction and is designed to understand and synthesize information across text, code, audio, images, and video. This versatility allows it to tackle many tasks, from content creation and media synthesis to more complex analytical tasks, with unprecedented efficiency.

"Google Gemini AI is our answer to the growing demand for AI that seamlessly integrates and interprets various data types," Deepak explains. He highlights Gemini AI's flexibility and efficiency, which make it a potent tool for developers and enterprises looking to harness AI across diverse platforms and devices.

Choosing the right AI for enterprises

There's no one-size-fits-all solution when selecting the appropriate large language model for enterprise use. The choice between ChatGPT and Gemini AI—or any other LLM—depends on many factors, including the business's specific needs, integration capabilities, cost considerations, and the desired balance between creativity and analytical prowess.

"Google Gemini AI might be the go-to for those requiring robust multimodal capabilities, particularly in STEM, law, or medicine," Deepak suggests. On the other hand, "OpenAI ChatGPT is unparalleled in creative and conversational applications, making it ideal for sectors like education, media, and customer service."

"We're looking at a future where LLMs, through their integration into various applications, will significantly enhance communication interfaces, making them more intuitive and efficient."

PRADEEPTA MISHRA
Co-Founder & Chief Architect,
Data Safeguard Inc.

"ChatGPT's natural language processing capabilities enable it to generate responses that can significantly enhance user interaction and satisfaction."

DEEPAK AGARWAL
Ex-Executive Director
Indian Oil Corporation

The road ahead

As AI continues to evolve, the distinctions between models like ChatGPT and Gemini AI will become increasingly nuanced, with each iteration bringing new capabilities and improvements. Agarwal's insights illuminate the current landscape and hint at a future where AI's potential is limited only by our imagination.

For enterprises, the journey towards AI integration is fraught with challenges but also brimming with opportunities. By understanding the unique strengths and limitations of models like ChatGPT and Gemini AI, businesses can better navigate the AI revolution, leveraging these powerful tools to innovate, enhance efficiency, and, ultimately, transform their operations for the digital age.

The future of LLMs

As we delve into the transformative potential of Large Language Models (LLMs) across various industries, Pradeepta Mishra, Co-Founder & Chief Architect at Data Safeguard Inc., known for his expertise in the field, emphasizes the dynamic nature of LLM development, influenced by technological advancements and ethical considerations.

"The transformative potential of LLMs lies not just in their ability to understand or generate text but in their capacity to bring about a paradigm shift in how businesses operate. We're looking at a future where LLMs, through their integration into various applications, will significantly enhance communication interfaces, making them more intuitive and efficient," Pradeepta explains. This statement underscores his belief in the power of LLMs to change the fundamental ways businesses engage with their customers and manage internal processes.

One of the key expectations Pradeepta highlights is the advancement in multimodal AI, allowing LLMs to process and combine various forms of data for a richer understanding of content. However, he doesn't overlook the ethical and regulatory challenges accompanying the widespread adoption of LLMs. Pradeepta advocates for industry-specific solutions, addressing sectors' unique needs, such as healthcare and finance, while stressing the importance of continued research, interoperability, and collaboration to mitigate security concerns and ensure responsible AI deployment.

Generative AI's role in manufacturing

Shweta Srivastava, head of IT for Matix Fertilisers and Chemicals Ltd, outlines practical applications of LLMs in production optimization, quality control, and predictive maintenance. Srivastav's detailed account of how LLMs can pre-empt equipment failures and optimize demand forecasting illustrates the tangible benefits of AI in enhancing productivity and cost control within the manufacturing sector.

Srivastava illustrates the transformative impact of LLMs, saying, "By integrating LLMs into our production and maintenance systems, we've been able to pre-empt equipment failures and significantly enhance our demand forecasting. This proactive approach reduces downtime and ensures we're operating at peak efficiency." This statement highlights the critical advantage of using AI to predict and solve problems before they impact production, demonstrating a shift from reactive to proactive management in manufacturing operations.

Moreover, Shweta points to the potential of computer vision LLMs in ensuring quality assurance on production lines and refining equipment operating parameters for optimal performance. Her insights underscore the role of LLMs in enabling manufacturers to adopt a proactive approach to planning and problem-solving, leading to improved efficiency and profitability.

Unified expectations and challenges ahead

Pradeepta and Shweta acknowledge the varied and complex expectations for LLMs across different organizational types and sectors. They concur on the innovation, productivity, and competitiveness LLMs can bring to organizations, fostering a culture of continuous learning and improvement. Nonetheless, they also caution against data privacy, security, ethics, and governance challenges, highlighting the need for a comprehensive LLM evaluation and implementation framework.

"By integrating LLMs into our production and maintenance systems, we've been able to pre-empt equipment failures and significantly enhance our demand forecasting. This proactive approach reduces downtime and ensures we're operating at peak efficiency."

SHWETA SRIVASTAVA
Head IT, Matix Fertilisers and Chemicals Ltd

As LLMs evolve, their potential to transform industries becomes increasingly evident. However, realizing this potential requires a balanced approach considering technological capabilities, ethical implications, and industry-specific needs.

Tips for CIOS

For Chief Information Officers (CIOs), implementing Large Language Models (LLMs) is both a strategic imperative and a complex challenge that demands meticulous planning and foresight.

GENAI can spark creativity and drive productivity across all lines of business. Goldman Sachs forecasts that GENAI can deliver a $7 Trillion boost in global GDP over the next 10 years. IDC estimates that India will be the third fastest AI-adopting country in Asia by 2026 after China and Australia.

Deepak Agarwal suggests a few tips to tips to get CIOs started using Gen AI:

- Your Data is a differentiator, so get your data house in Order.
- Include in your people along with your GENAI Journey. Cloud skills are essential since most GENAI cases require massive data and computing capacity.
- Work Backwards... First, understand the customer challenge, get the ideal solution, and build the product that solves the challenge.
- Build responsible and sustainable solutions.
- Select the right foundation model for the right use case
- Start small with PoV

Agarwal's strategic tips for navigating this new frontier emphasize the crucial role of data, the importance of a skilled and inclusive team, and the need for a methodical approach to innovation. This journey into GenAI is not just about technology; it's about pioneering a future where customer service, competitive edge, product development, and risk management are reimagined through the lens of generative artificial intelligence. ■

Cybersecurity challenges and how enterprises can fight the ever evolving threat

Cyber attacks are on the rise globally, with rise significant rise in the first quarter of 2024, almost 5% more than last time, marking an urgent need for updated ways to deal with the evolving challenges

By **Praneeta**

Check Point released its cybersecurity report for the first quarter of 2024. The report shed light on the evolving cybersecurity challenges that emerged in Q4 2024 and also discussed how far the enterprises are from solving AI-powered cybersecurity challenges.

According to Check Point, a software providing company, there was a significant rise in cyber attacks, with organizations facing an average of 1308 attacks per week. This is 5% higher than the same period last year and 28% higher than the previous quarter. This increase from Q4 2023 showcases the rise in attacks and also highlights the ever-evolving landscape of cyber threat and security.

Omer Dembinsky, Data Research Group Manager at Check Point Software, said, "As we witness the dynamic landscape of cyber threats in Q1 2024, it is clear that our approach to cybersecurity needs to be equally dynamic and proactive. The significant rise and volume of cyber attacks in regions like Europe, Africa, and particularly in North America, where 59% of the known ransomware attacks were concentrated, signals an urgent need for enhanced vigilance and robust cybersecurity measures."

"The startling 96% surge in ransomware attacks YOY on the Manufacturing sector and the unprecedented 177% increase YOY in the Communications sector are indicative of the vulnerabilities introduced by rapid digital transformation and the critical nature of these industries. These figures are not just statistics; they represent an urgent call for organizations across all sectors to bolster their defenses and prioritize cybersecurity, underscoring the need for adaptive, AI-powered defense strategies," he added.

Industry-wise data

According to the report, the Education sector experienced the most attacks, with an average of 2454 attacks per organization weekly, followed by the Government/Military sector with 1692 attacks per week and the Healthcare sector with 1605 attacks per organization.

However, what's concerning is the big jump in cyber attacks on hardware vendors. These attacks increased by 37% compared to last year. It shows that cyber criminals are targeting these companies more because they rely heavily on hardware for things like smart devices and the Internet of Things (IoT).

IBM X-Force Exchange, a cybersecurity threat intelligence team and platform operated by IBM, in its Threat Intelligence Index 2024, names Manufacturing as the top attacked industry in 2023 for the third year in a row, representing 25.7% of incidents within the top 10 industries year over year.

The finance and insurance industry was in second place, representing 18.2% of incidents. The share of attacks across the energy, retail and wholesale, healthcare, transportation, and arts, entertainment, and recreation sectors increased year over year.

The Communications sector saw a significant increase in attacks, likely due to rapid digital transformation and the integration of technologies like 5G and IoT.

Regional trends

According to the IBM XForce report in 2021 and 2022, the Asia-Pacific region was hit the hardest by cyber incidents, followed by Europe in second place. In 2023 Europe became the most affected region, making up 32% of incidents responded to by X-Force. North America accounted for 26% of incidents, Asia-Pacific for 23%, Latin America for 12%, and the Middle East and Africa for 7%.

However, in the first quarter of 2024, North America faced the highest impact from ransomware attacks, with 59% out of nearly 1000 reported

SHARE OF ATTACKS BY INDUSTRY 2019-2023

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and insurance	18.2%	18.9	22.4	23	17
Professional, business and consumer services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and telecommunications	1.2%	0.5	2.5	5.7	10

Source: IBM X-Force Threat Intelligence Index 2024 attacks, according to the Check Point report. Europe followed with 24%, and APAC with 12%. Europe experienced the largest increase in attacks compared to the same period in 2023, with a significant 64% rise.

This increase could be due to factors like increased digitization and regulatory environments that are making organizations more vulnerable. Meanwhile, North America saw a 16% increase, suggesting attackers continue to focus on this region.

These trends highlight the evolving cyber threat landscape and the need for robust cybersecurity measures to safeguard organizations and critical infrastructure.

Region	Percent out of Published Ransomware Attacks	YoY Change in Amount of Published Attacks
North America	59%	+16%
Europe	24%	+64%
APAC	12%	-13%
Latin America	4%	+14%
Africa	1%	+18%

Source: CheckPoint Report

What can enterprises do

Check Point suggests enterprises develop and adopt a multi-faceted approach to cybersecurity. Data backups, cyber awareness training, timely security patches, strong user authentication, and advanced anti-ransomware solutions are to be made a regular practice.

“Proactive engagement with AI-powered defenses can significantly bolster an organization’s resilience against these threats,” the report adds.

IBM states that to minimize the risk of credential harvesting attacks, enterprises should deploy Endpoint Detection and Response (EDR) tools across all servers and workstations in their environment. These tools help detect malware, including infostealers and ransomware and can identify abnormal behavior, such as data exfiltration or unauthorized account creation. They also suggest to consider leveraging experts to establish and operationalize threat hunting within your environment.

If resources are limited, consider using AI to manage up to 85% of alerts, allowing for 24/7 threat detection and response services. Additionally, it utilizes threat intelligence to identify opportunities for mitigating new threats. Strengthen credential management practices by implementing Multi-Factor Authentication (MFA) and robust password policies, including passkeys. Employ hardened system configurations to make accessing credentials more challenging.

Credential harvesting attacks often occur through phishing and watering hole attacks. Regularly educate employees on updated phishing techniques and scrutinize all third-party traffic. Treat third-party traffic as untrusted until verified. Watering hole attackers may exploit legitimate resources to deliver malware.

To reduce the cybersecurity blast radius, consider the potential impact of an incident on users, devices, or data. Implement solutions to minimize damage in case of a security incident, mainly focusing on data security and identity management.

IBM states that to minimize the risk of credential harvesting attacks, enterprises should deploy Endpoint Detection and Response (EDR) tools across all servers and workstations in their environment.

Conclusion

Cyber attacks are evolving rapidly, faster than enterprises can keep up. This is the right time to integrate AI and leverage AI-powered tools to counter the attacks and protect businesses and the people. Enterprises need to evolve with time and technology as well, using different methods and upskilling to help ward off the pesky attacks and malware. ■

Ensuring Secure Email Communications: The Power of Authentication

Despite the advent of instant messaging platforms and other tools, email continues to dominate the realm of professional correspondence.

By **Pramod Sharda**

In today's digital age, where email remains the cornerstone of communication for businesses and individuals alike, ensuring the security of email communications is paramount. Despite the advent of instant messaging platforms and other tools, email continues to dominate the realm of professional correspondence. However, the risks associated with email, such as phishing attacks, spam, and email fraud, underscore the urgent need for robust security measures.

The Power of Three: DKIM, SPF, and DMARC

Internet Service Providers (ISPs) employ three key technologies to bolster email security: DKIM (Domain Keys Identified Mail), SPF (Sender Policy Framework), and DMARC (Domain-based Message Authentication, Reporting, and Conformance). These technologies work synergistically to protect users from cyber threats and ensure the legitimacy of emails, mitigating the risk of fraudulent activities during transmission.

Understanding Email Authentication

Email authentication employs cryptographic techniques like digital signatures and encryption to verify the identity of senders and safeguard message content from manipulation. DKIM, SPF, and DMARC collaborate to create a comprehensive email authentication framework, enhancing the overall security of email communications.

Why Email Authentication Matters

- **Preventing Phishing Attacks:** Email authentication verifies the legitimacy of senders, thwarting phishing attempts where attackers impersonate trusted sources to deceive recipients into divulging sensitive information.
- **Protecting Brand Reputation:** By preventing cybercriminals from exploiting fake email addresses or domains, email authentication safeguards an organization's brand reputation from the detrimental effects of spam and phishing attacks.
- **Enhancing Email Security:** Authentication protocols like DKIM, SPF, and DMARC fortify email security by thwarting unauthorized access, tampering, and interception of messages, thereby ensuring confidential information remains protected.
- **Regulatory Compliance:** Compliance with industry regulations mandating email authentication is crucial to avoid penalties and legal ramifications, making the implementation of these protocols imperative for businesses across various sectors.

Organizations across industries must prioritize the configuration and maintenance of authentication systems like DKIM, SPF, and DMARC to bolster email deliverability and protect against malicious activities.

*–**Pramod Sharda,** CEO, IceWarp India and Middle East*

Conclusion

In conclusion, organizations across industries must prioritize the configuration and maintenance of authentication systems like DKIM, SPF, and DMARC to bolster email deliverability and protect against malicious activities. IceWarp emerges as the preferred choice for CIOs, backed by its track record of excellence and trustworthiness recognized through prestigious accolades like the CIO Choice Award. By implementing IceWarp, organizations can fortify their email environment with an additional layer of authentication, ensuring heightened security without compromising commercial flexibility. ■

Navigating the New Realities of Global Applications and Cybersecurity

Arul Elumalai, GM Security & Distributed Cloud (SDC) Product Group at F5, and **Shawn Wormke,** Vice President and General Manager of NGINX,- discuss recent trends, reflecting a comprehensive view of the current and future states of application development and cybersecurity.

By **Nisha Sharma**

The global application landscape has experienced a significant transformation catalyzed by advancements in digital technologies and an increasing emphasis on robust cybersecurity measures. This evolution presents opportunities and challenges for businesses as they adapt to a rapidly changing environment. Here, we delve deeper into the dynamics shaping this landscape, the complexities introduced by new technologies, and the strategies enterprises adopt to secure their digital assets.

In a recent exploration of the rapidly evolving global application landscape, Nisha Sharma engaged in a revealing conversation with Arul Elumalai, GM Security & Distributed Cloud (SDC) Product Group at F5, and Shawn Wormke, Vice President and General Manager of NGINX.

The discussion focused on the current challenges and advancements shaping how businesses approach digital transformation and cybersecurity. Arul provided insights into the strategic management of application demands within today's fast-paced digital economy. Shawn complemented this by discussing methods to enhance modern application deployment through innovative technologies. Together, their expert perspectives shed light on effective strategies for navigating the complexities of technological advancement and robust cybersecurity in an increasingly interconnected world.

ARUL ELUMALAI
GM Security & Distributed Cloud (SDC) Product Group at F5

The evolution of global applications

The number of applications enterprises utilize in the digital era has surged dramatically. This isn't just a quantitative increase but also a qualitative one, where applications have become more integral to business operations across various sectors and regions. The shift towards digital-first strategies has necessitated the modernization of application architectures, embracing microservices and distributed cloud environments to enhance agility and scalability.

"Across Big IP and NGINX, we are seeing a portfolio build-out that supports these modernized architectures, leading to further distribution and fragmentation of both applications and data," explained Arul Elumalai, GM Security & Distributed Cloud (SDC) Product Group at F5; this development underscores a broader industry trend towards decentralization, where applications are not just stored in a centralized data center but are spread across multiple cloud environments, from public to private and hybrid models.

Moreover, the rise of public-facing APIs has introduced new layers of complexity and vulnerability. APIs have become the backbone of digital interaction, facilitating data exchange and functionality between software applications. However, they also represent a significant security risk if not properly managed and secured, highlighting the need for comprehensive API security strategies.

Cybersecurity challenges and strategic responses

As applications become more complex and distributed, securing them becomes increasingly challenging. The fragmented nature of modern applications introduces numerous vulnerabilities, making traditional perimeter-based security measures insufficient. "Managing the risk associated with this distributed architecture is paramount, as each node and service within the system potentially opens up new avenues for attack," noted Shawn Wormke, Vice President and General Manager of NGINX.

SHAWN WORMKE
Vice President and General Manager of NGINX

Companies like F5 have developed distributed cloud platforms that integrate security directly into the application environment to address these challenges. This integration allows for consistent security policies across all applications, regardless of where they are deployed. It simplifies management and enhances the ability to respond to threats in real-time.

"By connecting applications across all environments with a secure network layer and embedding security services within, we can tame the complexity and ensure comprehensive protection," said Shawn Wormke. This approach is critical in an era where cyber threats are becoming more sophisticated and pervasive, as evidenced by the staggering number of cyber attacks reported annually.

The shift towards digital-first strategies has necessitated the modernization of application architectures, embracing microservices and disturbed cloud environments to enhance agility and scalability.

Future directions

Looking ahead, artificial intelligence (AI) and machine learning (ML) are set to play pivotal roles in shaping the future of application development and cybersecurity. These technologies offer the potential to automate complex processes, provide predictive insights, and enhance the efficiency of security protocols.

F5, for example, is integrating AI capabilities across its portfolio to offer advanced behavioral analysis, automate threat detection, and streamline management processes. "Our AI-driven tools are designed to not only detect and respond to threats in real-time but also provide predictive capabilities that help prevent incidents before they occur," shared Arul Elumalai at F5.

Moreover, as enterprises increasingly adopt AI-driven applications, the complexity of managing and securing these applications will escalate. Integrating AI into cybersecurity strategies is expected to mitigate these challenges by enhancing the intelligence and responsiveness of security systems.

Conclusion

The evolution of the global application landscape and the corresponding cybersecurity challenges require a nuanced understanding and a proactive approach. Enterprises must embrace innovative technologies and strategies to secure digital assets while fostering growth and innovation. ■

Balancing innovation and data security is critical for enterprises

Balakrishnan Kavikkal, CEO and co-founder of Autonom8 illuminates the integration of GenAI into the LCNC domain, setting new benchmarks for innovation, security, and efficiency in enterprise automation.

By **Nisha Sharma**

Integrating Generative Artificial Intelligence (GenAI) with Low-Code/No-Code (LCNC) platforms heralds a new era in software development, promising to minimize coding complexity and enhance business operational agility. This fusion aims to streamline enterprise automation, allowing for rapid deployment of customized processes and enhancing conversational interfaces. Amidst the benefits, it also raises crucial data privacy and security considerations, particularly in sensitive sectors.

Ensuring the safety of user data and maintaining compliance with regulatory standards is paramount, with strategies like data redaction, encryption, and rigorous API security measures in place. Understanding the balance between technological advancements and security implications becomes crucial as organizations navigate this innovative landscape.

In an insightful Q&A with Nisha Sharma, Principal Correspondent at CIO&Leader, Balakrishnan Kavikkal, CEO and co-founder of Autonom8, shares his perspectives on the challenges and opportunities presented by GenAI integration in LCNC platforms.

BALAKRISHNAN KAVIKKAL
CEO and Co-Founder, Autonom8

CIO&Leader: Autonom8 is recognized as the world's first GenAI-integrated LCNC platform. Can you share the journey and inspiration behind incorporating Generative AI into your platform?

Balakrishnan Kavikkal: We had two objectives when we started working with LLM models over two years ago. One was to reduce the amount of code needed to write (basically, to move further from Low-Code to No-Code), and the second was to augment our Conversational channels with GenAI integration.

Our target customers are mid-to-large enterprises. These enterprises have unique processes and several internal systems (CRM, ERP, Core). For any automation solution to work impactfully, it needs to be integrated with these systems and should be able to roll out its bespoke processes. With GenAI integration, these customizations can be done easily—with the co-pilot capability.

CIO&Leader: Speed and flexibility are highlighted as crucial USPs of Autonom8, along with the cost-effective utilization of Generative AI. How do these elements translate into tangible benefits for your clients?

Balakrishnan Kavikkal: Software projects/implementations are notorious for two things. The time it takes for an application to go live and the flexibility to easily make changes as your business requirements change. This is true even in Product implementations, as the process takes months and years. In our current times, we believe that customers need speed (the ability to go live quickly) and the flexibility to make changes as the business demands change. This is the Autonom8 value proposition. IT teams can respond to business needs faster, and customers can get significantly better ROI.

CIO&Leader: With the increasing focus on data privacy and security, how do you ensure the security and compliance of its platform, especially when handling sensitive information in the BFSI sector?
Balakrishnan Kavikkal: You are right. This is a critical issue. To protect user PII, we use various techniques such as redaction, encryption, and substitution.

From a compliance perspective, our SaaS platform offers many data sovereignty, encryption, and protection choices. The low-code platform enables rapid response to regulatory changes.

Additionally, for LLMs, we configure the platform to limit scope, creativity, and grounding (via dynamic prompts) to minimize misinformation.

CIO&Leader: Generative AI introduces new security risks, including data poisoning and adversarial attacks. What best practices should organizations follow to protect their AI models and sensitive data?
Balakrishnan Kavikkal: Model integrity can be protected with many of the same approaches as other IPs, such as code is protected. These include reviews, testing with different data types, data validation (e.g., not training on data with unknown provenance), etc. For training or fine-tuning, approaches such as regularization, MoE, over/under-sampling, etc., produce more resilient models. Finally, when deployed, models should be continuously monitored with reliable versioning & rollback strategies in place.

CIO&Leader: What advanced security measures and technologies are essential for industries handling sensitive information, such as BFSI, to protect customer data from breaches and unauthorized access?
Balakrishnan Kavikkal: We use three broad approaches to protect sensitive user information:

1. **Redaction:** Sensitive information (alphanumeric or image) is masked or redacted. This can also be supplemented with anonymization and differential privacy techniques.
2. **Encryption:** If the data needs to be communicated to the model and cannot be redacted, we can use encryption to transmit the data without in-flight risk
3. **Substitution:** In some instances, e.g., for proper nouns, names can be substituted so that the connection between PII and other data, e.g., bank balance, is not divulged

CIO&Leader: As companies increasingly rely on third-party services and APIs, what practices should be in place to assess and mitigate the security risks posed by these external entities?
Balakrishnan Kavikkal: The critical risks from third-party services include misinformation, response flooding, and misuse. In addition to vetting and auditing vendors, contractual provisions, and proper authentication and encryption, the following techniques will help mitigate security risks.

- **Input Validation and Sanitization:** Prevents common vulnerabilities like SQL injection, cross-site scripting (XSS), and command injection attacks.
- **Rate Limiting and Throttling:** Control the volume of requests to prevent abuse DoS attacks and maintain performance.
- **Monitor API Usage and Performance:** Detect anomalies in request volume, payload size, request sources, response time, error rate, etc., and trigger remedial action.
- **Patch Management:** Deploy security patches and updates released by the API providers. Review their documentation regularly and subscribe to security advisories or notifications to promptly address any security vulnerabilities.
- **Data Minimization:** Keep payloads lean to improve performance and reduce data exposure
- **Failover:** Implement fallback mechanisms or alternative solutions if the third-party API becomes unavailable. ■

Make goals, support, talk, and take risks for big changes

Sudhir Kanvinde, CIO at The Supreme Industries, outlines the importance of staying ahead of rapid technological advancements, the necessity of cybersecurity, and the impact of technologies like AI, cloud computing, and the Internet of Things (IoT).

By **Nisha Sharma**

The role of the CIO has expanded significantly in the rapidly evolving landscape of technology and digital transformation. It transcends the traditional confines of IT to become a linchpin in strategic business decision-making.

A recent discussion between Nisha Sharma, Principal Correspondent at CIO&Leader, and Sudhir Kanvinde, CIO at The Supreme Industries, delves into the milestones, challenges, and evolving strategies delineating the modern CIO's career trajectory.

Early career and shifts in focus

"The journey often starts in the technical trenches," Sudhir Kanvinde shares, reflecting on an early career in the production planning department for medical engineering equipment at Siemens. This trajectory highlights a crucial aspect of a CIO's path: the necessity to continually adapt, leveraging opportunities within and outside current roles to gain diverse experiences. "I started with proprietary technology for medical engineering equipment and moved through manufacturing with IT, to ERP implementations, and consulting within Siemens."

Navigating through government and private sectors

The capability to adapt and navigate the complexities of both the private and government sectors is pivotal. "I worked as an IT executive director for the Indian Forces under the Ministry of Ports, Shipping, and Waterways… My responsibility was to improve the digital and ease of doing business ranking of India."

Evolving role of the CIO

Over the last quarter-century, the CIO role has transformed from focusing on keeping the "lights on" to becoming a strategic business partner. "The role of CIO has evolved significantly in 25 years… from technology manager and head to strategic leader and innovator," Sudhir Kanvinde remarks. This reflects the broader recognition of IT as a critical driver of innovation, efficiency, and business growth.

Confronting and overcoming challenges

A CIO's journey is fraught with challenges, from staying ahead of technological advancements to cybersecurity risks. "The rapid technology development keeps the CIOs on their toes… Big data, AI, and cloud computing have changed the game." Overcoming these challenges requires a deep understanding of business needs, strategic technology implementation, and proactive security measures. "Involving business in the evaluation process ensures that tech solutions deliver real value. Set clear goals… evaluate, encourage, and communicate. Risk-taking ability is crucial for drastic changes."

Navigating remote work and the future of workplaces

The COVID-19 pandemic prompted widespread adoption of remote work. "Work from home is not encouraged unless necessary… high skill, high will can work from anywhere," the CIO notes, emphasizing the nuanced approach needed in adapting to new work environments.

The role of the CIO is crucial, demanding a blend of technical know-how, strategic vision, and leadership skills. "CIOs must remain at the forefront of innovation, guiding their organizations through digital transformation." As technology evolves, CIOs are pivotal in steering their businesses toward future success in the digital age, marking their journey as continuous growth, challenge, and opportunity. ■

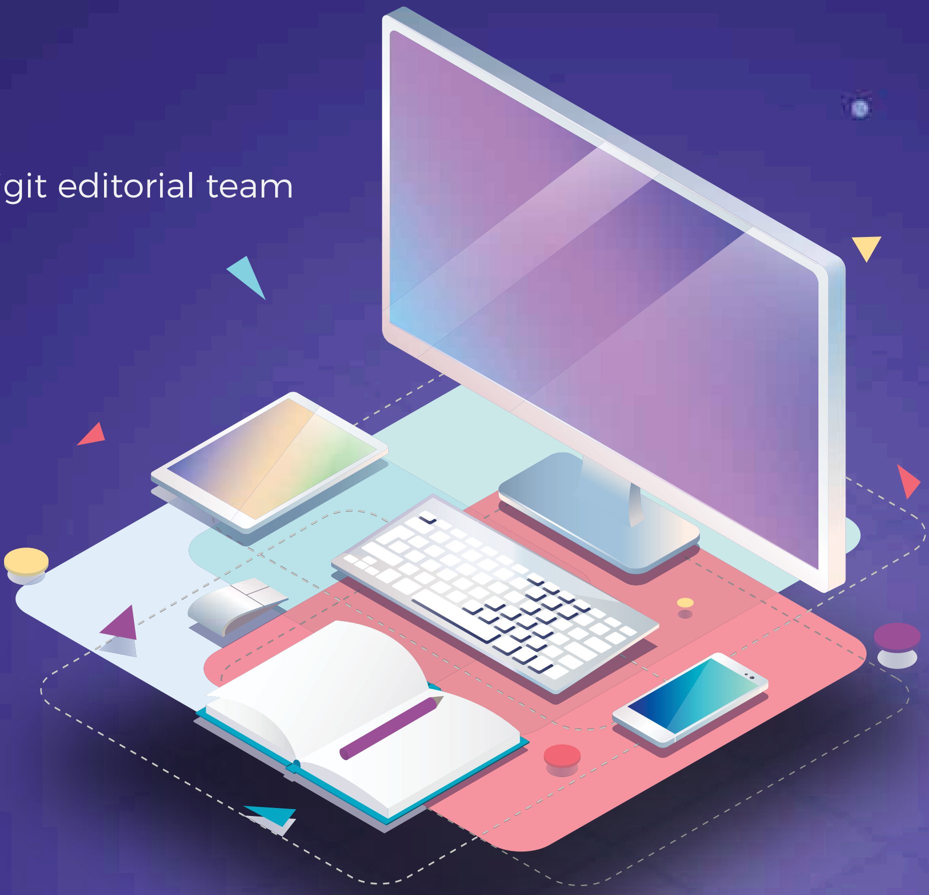
LAUNCHING

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