



Dawn of Generative AI: Can ChatGPT Overcome Privacy Concerns?



Sean Duca
Palo Alto Networks



Ramprakash Ramamoorthy
ManageEngine



Satnam Narang
Tenable



Reuben Koh
Akamai Technologies



Dhananjay Ganjoo
F5



Ranga Jagannath
Agora



Jhilmil Kochar
CrowdStrike India

SAMSUNG

Find the perfect book for your business



Galaxy Book2 Series

The new way to PC



Samsung recommends Windows 11 Pro for Business

Follow us on: [samsung.com](https://www.samsung.com) | [@SamsungIndia](https://www.facebook.com/SamsungIndia) | [@SamsungIndia](https://www.twitter.com/SamsungIndia) | [SamsungIndia](https://www.youtube.com/SamsungIndia) | [@samsungindia](https://www.instagram.com/samsungindia)



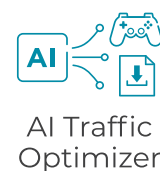
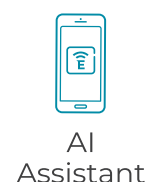
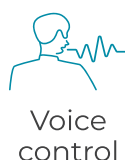
Please dispose of e-waste and plastic waste responsibly.
For more information or for e-waste pick up, please call 1800 40 7267864 or 1800 5 7267864.

Image simulated for representational purposes only. Colours as per the availability. S Pen is sold only with Galaxy Book2 Pro 360.
Windows and Microsoft and their logos and images are trademarks/ registered trademarks of Microsoft Corporation. Intel Evo available in select models. Intel, Intel Evo and their logos and images are trademarks/ registered trademarks of Intel Corporation.



Scan to
experience

Does your Wi-Fi have the power of



Get the EAGLE PRO AI Series in your home and experience
the power and convenience of AI powered Wi-Fi.

EAGLE PRO AI

One Connection - Infinite Possibilities

Wi-Fi 6



AX1500
Smart
AI Router



M15 (Pack of 2)
AX1500
AI Mesh System

11AC



R12
AC1200
Smart AI Router

N300



R04
N300 AI Router
(3 antennas)



R03
N300
AI Router



For details: ✉ sales@in.dlink.com

Scan the QR code
to explore more about
D-Link Eagle pro AI Series



Contact D-LINK (INDIA) LIMITED

- KOLKATA:** Mr. Somnath Ghosh - Ph.: +91-7506513344, E-mail: somnath.ghosh@in.dlink.com
- GUWAHATI:** Mr. Ashish S - Ph.: +91-91364 76280, Email: ashish.singhania@in.dlink.com
- BHUBANESWAR:** Mr Saumya Pradhan Ph.: +91-97774 11922, Email: saumya.pradhan@in.dlink.com

CONTENT

COVER STORY

6



Dawn of Generative AI: Can ChatGPT Overcome Privacy Concerns?

IN CONVERSATION

ChatGPT Holds the Potential to Lower the Technical Bar for Attackers: Palo Alto Networks



15

SEAN DUCA, VP, Regional Chief Security Officer - Asia Pacific & Japan, Palo Alto Networks

Real-Time Engagement Plays a Significant Role in the Adoption of Generative AI: Agora



19

RANGA JAGANNATH, Senior Director, Agora

Businesses need to be Wary of Loopholes in OpenAI's Data Collection and Sharing: ManageEngine



21

RAMPRAKASH RAMAMOORTHY
Director, AI Research, ManageEngine

CHANNEL NEWS 23-27

- Micron Technology Inc Forecasts 60% Revenue Drop in Q3, Plans for a Record 2025 with AI Boosting Sale
- Zscaler Appoints Karl Soderlund as Senior Vice President, Worldwide Partners, and Alliances
- Salesforce Launches Generative AI for CRM, Einstein GPT
- UiPath Integrates Automation Workflows with Amazon SageMaker to Amplify ML Models
- CONVOKE: ALOGIC Strengthens its Partnerships with a Dedicated Partner Meet in Mumbai
- Redington Partners with Indusface to Strengthen Application Security for Enterprises
- Tech Mahindra Appoints Mohit Joshi as MD & CEO Designate, Poised to Take Over in 2023
- Volante Technologies and HCLTech Forge Strategic Alliance to Unlock Financial Innovation
- ManageEngine Unveils Security & Risk Posture Management Dashboard for Comprehensive SIEM Solution.

CASE STUDY 28

Linksys and Fortinet Announce Strategic Alliance to Deliver Enterprise-Grade Performance and Security for Work From Home Networks



INSIGHT 29

UBS-Credit Suisse Merger and US Banking Troubles to Impact India's IT BPM Industry

Toner Box Series

Smartest choice for your business.

brother
at your side

**WHY COMPROMISE, WHEN YOU HAVE A CHOICE.
CHOOSE GENUINE. SAY NO TO NON-GENUINE.**

GET QUALITY, WARRANTY, DURABILITY, LONGEVITY.



With
ORIGINAL TONER COST

33 Paise*
Per Page

2600
PAGES YIELD



TONER TNB021

₹940
MRP



34 Pages
Per Minute



Duplex
Printing



250 Sheets
Paper Tray



2,600 Pages
Inbox Toner



Cost Saving
Toner Box Technology

SUPERIOR RANGE OF MONO LASER PRINTERS



PRINT | SCAN | COPY

DCP-B7535DW
MRP ₹ 25,290/=-



PRINT

HL-B2080DW
MRP ₹ 15,990/=-



PRINT | SCAN | COPY

DCP-B7500D
MRP ₹ 18,990/=-



PRINT

HL-B2000D
MRP ₹ 13,990/=-



PRINT | SCAN | COPY | FAX

MFC-B7715DW
MRP ₹ 26,990/=-

www.brother.in

FOR SALES ENQUIRIES: • **WEST BENGAL & ASSAM** : Raja Banerjee - 9007135395 / Soumavo Nandi - 8583010825, • **BIHAR** : Deepak Singh - 9771403031 / Amit Kumar - 9308475768, • **ORISSA** : Saroj Nayak - 9438362634, • **JHARKHAND** : Dilip Santra - 9334794315

*T&C Apply | Original toner cost per page is calculated on toner yield of 2600 pages (as per ISO/IEC 19752) at ₹846 | MRP mentioned above is for 1*unit and subject to change without prior notice



Dawn of Generative AI: Can ChatGPT Overcome Privacy Concerns?

Generative AI tools like ChatGPT have taken the world by storm. Within two months of its release, ChatGPT reached 100 million active users, making it the fastest-growing consumer application ever launched. However, recently it has been in news around the potential privacy risks ChatGPT poses for users and businesses. As AI capabilities continue to evolve, technology companies are getting locked into a fierce arms race. The problem is, this race is fuelled by our personal data

Amit Singh

If you have been following the recent news or scanning through your social media feed, then you must have noticed the rage of the hour: ChatGPT. Since its debut in November last year, ChatGPT has been attracting headlines for its

highly anticipated potential, which—depending on your view of artificial intelligence (AI)—will either transform work for the better by helping us with mundane and complicated tasks or will encroach disastrously into territory best navigated by

humans.

Owing to its chat box format, ChatGPT allows users to request information on highly specific topics—from quantum computing and processing code to the mechanics of the human heart or the principles of

flower arrangement. In this manner, it mimics the question-and-answer format of Google search, although instead of producing multiple answers on a search engine results page, ChatGPT acts as the sole authority delivering responses.



"The text-based AI bot is showcasing the immense power of AI to open a world of amazing new abilities, including fixing a coding bug, generating cooking recipes, creating 3D animations, and even composing songs. At the enterprise level, we are seeing companies integrating ChatGPT into their operations to improve automation in critical domains such as customer experience, online education, content creation, data analysis, and more," says Sean Duca, Vice President, Regional Chief Security Officer - Asia Pacific & Japan, Palo Alto Networks.

Furthering its capabilities, the Microsoft-backed startup OpenAI recently launched GPT-4, which builds on ChatGPT's wildly successful technology. Enhanced capabilities of the new model include the ability to generate content from both image and text prompts. Furthermore, GPT-4 scored 40 percent higher on factual accuracy tests and 82 percent less likely to respond to disallowed content requests than its predecessor. GPT-4 can also deal with longer documents of up to 25,000 words.

There is no doubt that ChatGPT will have

a significant impact on how humans will work in the future. However, with opportunities, there are privacy risks associated with using ChatGPT.

In fact, Italy has become the first country to block the advanced chatbot temporarily, saying it has improperly collected and stored information. Italy's privacy watchdog, Garante, charged Microsoft-backed OpenAI with failing to verify the age of ChatGPT's users who are required to be aged 13 or above.

According to Garante, ChatGPT lacks any legal justification for the extensive gathering and storage of personal data needed to train the chatbot. OpenAI has 20 days to react with corrective measures; otherwise, it runs the risk of being fined up to 20 million euros (\$21.68 million), which is equal to 4% of its annual global turnover.

Privacy risks

If you've ever written a blog post or product review or commented on an article online, there's a good chance this information was consumed by ChatGPT.

"More than 300 billion



“OpenAI has fed ChatGPT with over 300 billion words from data sets across the internet, including personal information obtained without consent. Considering the large amounts of data the platform already possesses, users are never asked if ChatGPT can use their data, which raises privacy concerns.”

SEAN DUCA, VP, Regional Chief Security Officer - Asia Pacific & Japan, Palo Alto Networks



words have been fed to ChatGPT by OpenAI from data sets collected from books, articles, websites, and posts on the internet, including personally identifiable information acquired without permission. Considering the large amounts of data the platform already possesses, users are never asked if ChatGPT can use their data, which raises privacy concerns. What's more, ChatGPT currently offers no means for users to check whether the company stores personal information or even deletes any previously shared information. Threat actors can easily take advantage of any underlying vulnerabilities in the platform to gain access to this sensitive data and use it for malicious purposes," highlights Duca of Palo Alto.

Generative AI tools like ChatGPT can collect personal information without the user's consent, such as IP addresses, browser types and settings, email addresses, and other contact information, and use this data to personalize the user's experience and target ads to them.

Another possible privacy

risk, according to experts, relates to the information that ChatGPT receives from user prompts. When we interact with the tool, we could inadvertently put sensitive information in the public domain without realizing it.

Moreover, OpenAI offers no procedures for individuals to check whether the company stores their personal information, or to request it is deleted. This is assured under the European General Data Protection Regulation (GDPR) - although it's still not clear if ChatGPT is compliant with GDPR requirements.

"OpenAI did state that it crawls millions of websites containing private information to collect training data. Additionally, there is still the matter of contextual integrity, which is the idea that personal information shouldn't be disclosed outside of the initial context in which it was given," states Ramprakash Ramamoorthy, Director, AI Research, ManageEngine.

Even when data is publicly available, its use can violate the principle of contextual integrity- a fundamental concept in



“OpenAI did state that it crawls millions of websites containing private information to collect training data. Additionally, there is still the matter of contextual integrity, which is the idea that personal information shouldn't be disclosed outside of the initial context in which it was given.”

RAMPRAKASH RAMAMOORTHY,
Director, AI Research, ManageEngine



discussions pertaining to privacy. Contextual integrity ensures that individuals' data is not disclosed outside of the context in which it was

initially created or collected.

The platform generates responses to user queries, which may include



“ Hoping to cash in on the massive interest around OpenAI's GPT-4, scammers have launched phishing campaigns via email and Twitter designed to steal cryptocurrency. ”

SATNAM NARANG,
Senior Staff Research Engineer, Tenable



“ The current immediate risks where ChatGPT can potentially be abused to improve attacks are in areas such as phishing and social engineering attacks, which continue to be a thorn on every security practitioner's side. ”

REUBEN KOH, Director,
Security Technology & Strategy, APJ, Akamai Technologies

copyrighted or trademarked material. ChatGPT does not own any of the intellectual property rights associated with these responses, and users must obtain proper permissions before using any

copyrighted or trademarked material generated by the platform

Multiplying the risk, there's a possibility of ChatGPT being misused to track the user's activities and



preferences or even being used to commit identity theft or phishing scams.

Identity theft/phishing scams

ChatGPT's ability to mimic language to a high degree of fluency, and incorporate the idioms of nationality, will surely be exploited by hackers for phishing attacks via email or text. Currently, the stilted language used in these attacks makes them easy to spot, but ChatGPT could make it easier for criminals to send out emails that come across as trustworthy and authoritative. The utility could also be used by hackers to create malicious code.

In fact, real-life use cases of ChatGPT being used for phishing have already surfaced. A team representing Singapore's Government Technology Agency at the Las Vegas Black Hat and Defcon security conferences recently demonstrated AI's ability to craft better phishing emails and effective spear phishing messages than humans. "Researchers combined OpenAI's GPT-3 platform with other AI-as-a-service products,

focused on personality analysis, and generated phishing emails customized to the backgrounds and characters of their colleagues. Eventually, the researchers developed a pipeline that groomed and refined the emails before hitting their targets," shares Duca of Palo Alto.

"We're seeing ChatGPT itself being used to improve the templates for phishing emails as well as attempts to steal cryptocurrency from users seeking to access GPT-4. Hoping to cash in on the massive interest around OpenAI's GPT-4, scammers have launched phishing campaigns via email and Twitter designed to steal cryptocurrency," adds Satnam Narang, Senior Staff Research Engineer, Tenable.

While ChatGPT is probably still some ways away from revolutionizing cyber-attacks, it certainly has the ability to make attacks more efficient, accurate, and impactful. The immediate risks right now are those related to phishing and social engineering attacks, which continue to be a pain in the neck for security professionals. ChatGPT has the potential to be used in these situations to enhance attacks, shares Reuben Koh,



“Creating employee awareness of the associated risks, having a response plan in place, and conducting regular security audits, are some important proactive measures”

DHANANJAY GANJOO,
Managing Director, India & SAARC, F5

Director, Security Technology & Strategy, APJ, Akamai Technologies.

Further, ChatGPT can serve as an upgrade to malware as a service, which has existed for some time now. There



are security risks associated with using these generative AI models to create more authentic phishing emails or automate the generation of malicious codes, which could result in many uninitiated users testing these methods as quick and simple ways to launch cyber-attacks, shares Jhilmil Kochar, Managing Director, CrowdStrike India.

User awareness is crucial

It is often challenging to pinpoint who is responsible for the actions of a generative AI system. The negative impacts of the system may be difficult to address due to this lack of accountability. However, this also means people must become more vigilant and guardrails have to get higher.

Users need to be cautious while granting permissions to the application and should be aware of the risks related to sharing personal data. "In addition, employees using ChatGPT within their network can lead to data breaches, making it crucial for organizations and their security teams to be prepared to battle this

threat. Creating employee awareness of the associated risks, having a response plan in place, and conducting regular security audits, are some important proactive measures. A proactive approach can reduce the potential risk associated with ChatGPT and other AI platforms," says Dhananjay Ganjoo, Managing Director, India & SAARC, F5.

From an employee perspective, data privacy can be one of the biggest concerns. If an employee is using ChatGPT for work, they should always verify the information received. Inaccurate or unreliable content can always find its way and set a wrong context adds Ranga Jagannath, Senior Director, Agora.

Narang of Tenable opines that it's less about permissions and more about what data users share with these generative AI services. "It can't be understated just how important it is for users to recognize that the information they share with services like ChatGPT helps to improve its model in future iterations."

Organizations must ensure that individuals are fully informed about how



“From an employee perspective, data privacy can be one of the biggest concerns. If an employee is using ChatGPT for work, they should always verify the information received. Inaccurate or unreliable content can always find its way and set a wrong context.”

RANGA JAGANNATH,
Senior Director, Agora

Here is what ChatGPT says about its features and measures around security and privacy:

← → ↻ chat.openai.com/chat

+ New chat

OpenAI Data Privacy. ✎ 🗑

AM Can bad actors and cyber criminals use ChatGPT to generate malicious codes, phishing, and malware campaigns?

It is possible for bad actors and cybercriminals to use language models such as ChatGPT to generate malicious codes, phishing, and malware campaigns. However, OpenAI takes steps to prevent the misuse of its language models, including ChatGPT, and has implemented safeguards to detect and prevent the generation of harmful or malicious content.

OpenAI restricts access to its language models to approved users who have undergone a rigorous vetting process, and closely monitors their usage for any suspicious or unauthorized activity. It has also implemented filters and controls to detect and block the generation of certain types of content, such as personal information or sensitive topics.

Despite these measures, it is still possible for malicious actors to attempt to use language models like ChatGPT for malicious purposes. This underscores the importance of practicing good cybersecurity hygiene, such as keeping software up-to-date, using strong and unique passwords, and being vigilant for suspicious activity or messages.

It is worth noting that OpenAI is committed to working with law enforcement and other authorities to investigate and prevent the misuse of its technology in illegal or malicious activities. If you come across any suspicious or harmful content generated by ChatGPT, you can report it to OpenAI or law enforcement authorities.

← → ↻ chat.openai.com/chat

+ New chat

OpenAI Data Privacy. ✎ 🗑

AM What are the specific measures OpenAI has taken to prevent misuse of ChatGPT in malicious, phishing, and malware campaigns?

OpenAI takes the responsible use of its AI technology very seriously and has put in place measures to prevent the misuse of its language models, including ChatGPT, in malicious activities such as phishing and malware campaigns. 🍏

One of the primary measures OpenAI has taken is to limit access to its language models, including ChatGPT, to approved users who have undergone a rigorous vetting process. OpenAI also monitors the use of its language models for any suspicious or unauthorized activity, and has the ability to shut down any usage that violates its terms of service or poses a security risk.

Additionally, OpenAI has implemented safeguards within ChatGPT itself to prevent the generation of content that could be used for malicious purposes. For example, it has trained ChatGPT on a diverse range of topics and language styles to reduce the likelihood of generating text that is explicitly harmful or offensive. It has also implemented filters and controls to detect and block the generation of certain types of content, such as personal information or sensitive topics.

OpenAI also works closely with law enforcement and other authorities to investigate and prevent the misuse of its technology in illegal or malicious activities.

Overall, OpenAI is committed to the responsible use of its AI technology and takes active steps to prevent its misuse. It continually evaluates and updates its measures to ensure the security and integrity of its language models, including ChatGPT.

🗑 Clear conversations

👤 Upgrade to Plus NEW



Inherent security measures

The European Union Agency for Law Enforcement Cooperation, better known as Europol recently said that while ChatGPT had safeguards including content moderation, which will not answer questions that have been classified harmful or biased, these could be circumvented with clever prompts.



OpenAI evaluated GPT-4 for a wide range of risks such as hallucination and harmful content and claim that it is

82 percent less likely to respond to questions that are not allowed and reduce false positives. Plus, it reduces the volume of toxic comments from 6.48 percent of requests to 0.73 percent for GPT-3.5. A red team of 50 experts has helped spot issues and risks, and the model comes with an extensive model scorecard highlighting these. Peter van der Putten, Director AI Lab, Pegasystems & Assistant Professor, Leiden University.

← → ↺


chat.openai.com/chat

+ New chat

OpenAI Data Privacy.  

AM

What is OpenAI's policy for data collection and sharing, including the user's IP addresses and the on-site interactions that take place?




As an AI language model, I don't have access to the current policies of OpenAI. However, I can tell you that OpenAI takes data privacy and security very seriously and is committed to protecting the privacy of its users.

OpenAI has a comprehensive privacy policy that outlines its practices for data collection and sharing. According to the policy, OpenAI collects certain information about users, including IP addresses and on-site interactions, in order to improve its services and provide a better user experience. This information may be shared with third-party service providers or used to fulfill legal obligations.

OpenAI also employs various technical and organizational measures to ensure the security of user data, including encryption and access controls. Users can also request to have their data deleted or to receive a copy of their data by contacting OpenAI's support team.

It's important to review OpenAI's current privacy policy for up-to-date information on its data collection and sharing practices.





their data is used and that all data is collected and used with explicit consent. Strong security measures should also be implemented to prevent unauthorized access to or disclosure of personal data, and organizations should be prepared to notify the concerned parties in the event of a data breach, says Ramamoorthy of ManageEngine.

He further adds that along with legal compliance, the ethical ramifications of generative AI must be taken into account, and measures must be taken to guarantee that the technology is used in

a transparent, accountable, and responsible manner. Also, generative AI models can be audited regularly to make sure they are being utilized properly. This will help build clear standards and procedures for the responsible use of generative AI.

Kochar of CrowdStrike shares that the best way for enterprises to deal with these challenges is to increase their focus on cybersecurity, invest in threat hunting, and use ML-based next-generation AV/ EDR. "ChatGPT is experimental and in its early stages at this time. While



“ ChatGPT is experimental and in its early stages at this time. As it progresses to further advanced versions, it is yet to be seen whether this develops into an alarming tool. **”**

JHILMIL KOCHAR,
Managing Director, CrowdStrike India



there are privacy and ethical concerns on one hand, there are cybersecurity concerns on the other. As it progresses to

further advanced versions, it is yet to be seen whether this develops into an alarming tool,” she states.



SEAN DUCA

VP, Regional Chief Security Officer,
Asia Pacific & Japan, Palo Alto Networks

ChatGPT Holds the Potential to Lower the Technical Bar for Attackers: Palo Alto Networks

Sean Duca, Vice President, Regional Chief Security Officer, Asia Pacific & Japan, Palo Alto Networks, states that ChatGPT holds the potential to lower the technical bar for attackers which may lead to an increased incidence of user-focused or social engineering cyber attacks. In a quick conversation with Amit Singh, he highlights that granting excessive permission to AI platforms without fully understanding the scope of the access can result in personal data being exposed or misused by the platform

■ **ChatGPT has become the fastest-growing consumer application ever launched with over 100 million active users within two months of its release. How do you see ChatGPT changing how humans work?**

Our efforts to decipher and mimic the human mind and natural thought led to the creation of Artificial Intelligence (AI). ChatGPT is the latest tool making headlines for its application of AI. From accurately fixing a coding bug, generating cooking recipes, and creating 3D animations to composing entire songs, the text-

based AI bot is showcasing the immense power of AI to unlock a world of incredible new abilities. We are already seeing cases of individuals using it to improve the effectiveness of their work processes and to access knowledge and ideas on various subjects, similar to the function of the Google search engine. At the enterprise level, we are seeing companies integrate ChatGPT into their operations to improve automation in critical domains such as customer experience, online education, content creation, data analysis, and more. It is evident that ChatGPT if used effectively, holds great potential to improve, simplify, and optimize our

personal and professional lives.

What privacy risks does it pose to users due to its ability to collect personal data?

ChatGPT is based on a Large Language Model (LLM) that relies on digesting large amounts of data to function and improve. To use the platform, members need to create detailed prompts or questions across levels of complexity to get the specific answers or solutions that they need. OpenAI, the company behind it, has fed the tool some 300 billion words from data sets across the internet: books, articles, websites, and posts - including

personal information obtained without consent. Now, considering the large amounts of data the platform already possesses, users are never asked if ChatGPT can use their data, which raises privacy concerns. What's more, ChatGPT currently offers no means for users to check whether the company stores personal information or even deletes any priorly shared information. Threat actors can easily take advantage of any underlying vulnerabilities in the platform to gain access to this sensitive data and use it for malicious purposes. The platform also collects a range of personal information on IP addresses,

Cont'd on page 18



KONICA MINOLTA

EXPERIENCE THE COLOURFUL TRANSFORMATION RETHINK COLOURS

RETHINK INTELLIGENT INNOVATIONS FOR WORKPLACE






PRINT | COPY | SCAN

A3 Colour & Mono Multifunctional Printers **bizhub i-Series**

For more information: SMS "KM MFP" send to 52424 or Call: 1-800-266-2525.

Konica Minolta Business Solutions India Pvt. Ltd.

www.konicaminolta.in | marcom@bin.konicaminolta.in

Connect with us:     

Giving Shape to Ideas



TRANSCON ELECTRONICS PVT. LTD.

205, 2nd Floor, Center Point Building, Hemanta Basu Sarani,
Opp. Lalit Great Eastern Hotel, Kolkata - 700001
Ph.: 22488118, 22488210, 22481620,
Mobile: +91-8337071326, Fax: 03322486604
Email: abhishek@transconelectronics.com,
Website: www.transconelectronics.com

browser types, settings, as well as interaction patterns with the site, which is likely to be shared with unspecified third parties.

■ What are the real-life possibilities of ChatGPT being misused to commit identity theft or phishing scams?

Real-life use cases or examples of ChatGPT being used for phishing have already surfaced. A team representing Singapore's Government Technology Agency at the Las Vegas Black Hat and Defcon security conferences recently demonstrated AI's ability to craft better phishing emails and effective spear phishing messages than humans. Researchers combined OpenAI's GPT-3 platform with other AI-as-a-service products, focused on personality analysis, and generated phishing emails customized to the backgrounds and characters of their colleagues. Eventually, the researchers developed a pipeline that groomed and refined the emails before hitting their targets. To their surprise, the platform also automatically supplied specifics, such as mentioning a Singaporean law when instructed to generate content for people in Singapore. While the makers of ChatGPT have suggested that the AI-driven tool has inbuilt guardrails designed to prevent any kind of criminal activities, with a few tweaks, it generated a near-flawless phishing email that sounded 'weirdly human.' This is evidence that ChatGPT holds the potential to lower the technical bar

for attackers which may lead to an increased incidence of user-focused or social engineering cyber attacks.

■ What are the security measures offered by ChatGPT? Are they enough to safeguard user privacy and data?

ChatGPT itself does not offer security measures as a part of its platform. However, the platforms or applications that integrate ChatGPT as a feature may implement security measures to protect user data and privacy. Here are some of the security measures that could be implemented to ensure the secure usage of ChatGPT:

- Encryption: Like chatting apps, the data exchanged between the user and ChatGPT could be encrypted to prevent unauthorized access.
- Authentication: Users could be required to authenticate themselves before accessing ChatGPT to prevent unauthorized access.
- Access controls: Access controls could be implemented to ensure that only authorized personnel can access the data stored by ChatGPT.
- Data minimization: The amount of data shared with ChatGPT could be minimized to reduce the risk of data breaches or leaks.
- Regular security updates: The platform or application that integrates ChatGPT could regularly update its security measures to address any new threats.

Overall, the security

measures implemented depend on the platform or application that integrates ChatGPT, and the specific requirements of that platform or application.

■ What are the major mistakes people commit while granting permissions or while using these kinds of AI platforms?

Per Palo Alto Networks and Unit 42's Cloud Threat Report, 99 percent of cloud identities are overly permissive and grant permissions that are never used. 62 percent of organizations surveyed even have publicly exposed cloud resources. This opens the door for malicious actors to have wider access to cloud environments. Similarly, granting excessive permission to AI platforms without fully understanding the scope of the access can result in personal data being exposed or misused by the platform. Additionally, ignoring privacy policies before granting permissions or using an AI platform can lead to misunderstandings about how the platform uses one's data and what rights they have to control it. Failing to update permissions or not revoking them where necessary can result in data being unnecessarily stored by the platform or being accessed by unauthorized parties. Understanding that AI is only as good as the data it is trained on and may make mistakes or produce biased outcomes if the data is flawed is crucial. It is also important for users to be aware of the risks associated with granting permissions or using AI platforms and with

taking steps to protect their data and privacy.

■ How are enterprises and security teams gearing to fight against any unforeseen disaster arising due to ChatGPT in their organization?

The conversation on using AI tools more responsibly and ethically will gain importance as ChatGPT grows. Governments around the world are establishing advisory bodies and teams to look at the technology holistically, along with the ethical impacts and the efficacy of these tools in certain deployments, including cybersecurity. For instance, the Organization for Economic Cooperation and Development (OECD) has developed a user-friendly framework to classify AI systems comprehensively. This framework is based on the OECD AI principles that include human rights, privacy and fairness, safety, security & risk assessment, transparency & accountability, and international cooperation.

Establishing such corporate policies and frameworks will be critical to doing business ethically while improving cybersecurity. Additionally, finding the right balance between our social values and economic interests will help firms tackle the complex legal, security, and ethical issues related to the potential risks of AI. While this will not be an easy task for policymakers when considering new legislation, it is clear that any successful coexistence of AI and humans will largely depend on robust cybersecurity practices.



RANGA JAGANNATH
Senior Director, Agora

Real-Time Engagement Plays a Significant Role in the Adoption of Generative AI: Agora

Ranga Jagannath, Senior Director, Agora in a quick conversation with Amit Singh shared that real-time engagement of AI tools enables humans to function faster due to rapid response time, hence improving their efficiency in performing a task. AI-based tools can provide valuable insights into the effectiveness of live voice and video communication by analyzing both verbal and nonverbal cues

■ **ChatGPT has become the fastest-growing consumer application ever launched with over 100 million active users within two months of its release. How do you see ChatGPT changing how humans work?**

Despite being only a few months old, ChatGPT has already caused ripples for both organizations as well as individuals. The biggest benefits of ChatGPT are the automation of tasks, quick and accurate responses to a wide range of questions and assistance with a wide range of tasks that require the understanding and generation of natural language. With the help of ChatGPT, one can get redundant tasks done easily, getting more time to focus on creative, complex, and critical tasks. ChatGPT gets access to a fair share of data, which helps humans in making more informed decisions with the help of analysis.

AI and automation are changing the nature of employment and the skills required for them, revolutionizing how humans work. AI is employed in various industries, including gaming, healthcare, banking, retail, and transportation. Technology is altering operations by increasing efficiency, lowering costs, and enabling new types of innovation. ChatGPT might not create a revolution but will increase human

efficiency manifold.

■ **What are the implications of its usage in the organizational network and what are the precautions employees need to take to avoid any uncomfortable situation?**

Organizations can benefit exponentially from adopting ChatGPT. Businesses can use it

perspective, data privacy can be one of the biggest concerns. Any information shared must comply with the organization's policies as confidential/sensitive information can be used in unintended ways. It's a good practice to use secure networks to prevent unauthorized access to any information. Also, if an employee is using ChatGPT for work, they should always verify the information received. Inaccurate or unreliable

inventory management, supply chain metrics, and more through new offerings in AI and predictive algorithms by digital service aggregators, has been vital to this acceleration. The real-time insights they offer allow organizations to deliver increased personalization and tailor their portfolios to the needs of the quickly evolving consumer. AI can help compete against larger organizations by improving their products, services, and customer engagement.

Real-Time Engagement (RTE) has a significant role to play here. Conversational AI tools respond to consumer inquiries instantly by understanding the context of inquiries better in a real-time environment, which helps in giving tailored responses. Moreover, RTE enables humans to function faster due to rapid response time, hence improving their efficiency in performing a task. AI-based tools can provide valuable insights into the effectiveness of live voice and video communication by analyzing both verbal and nonverbal cues. Features like speech-to-text analysis, sentiment analysis, and attention tracking facilitate better communication. One can easily understand the tonality of a conversation with these tools that rely on AI. The level/intensity of engagement can also be detected with these tools, giving a better insight into what worked and what did not.

“The biggest benefits of ChatGPT are the automation of tasks, quick and accurate responses to a wide range of questions and assistance with a wide range of tasks that require the understanding and generation of natural language.”

for seamless customer support and take assistive technology to a new level. Automation of customer support will become more cost-effective and efficient. The potential is not just limited to support. By analyzing interactions, businesses can gain insight into consumer behavior (data analysis). They can also use personalized marketing tactics, tailored for every user which can help with retention.

While the benefits of an AI language model are huge - for the employers and employees - there are significant risks involved. From an employee

content can always find its way and set a wrong context.

■ **Why are organizations increasingly adopting ChatGPT and other AI technologies? How do you see real-time engagement play a role in this?**

The rapid acceleration towards digitalization during the pandemic has helped even the smallest enterprises transform their businesses. Accessing analytics dashboards for critical insights into customer behavior,

**RAMPRAKASH RAMAMOORTHY**

Director, AI Research, ManageEngine

Businesses need to be Wary of Loopholes in OpenAI's Data Collection and Sharing: ManageEngine

Ramprakash Ramamoorthy, Director, AI Research, ManageEngine, puts the responsibility on the users when it comes to the data they share on generative AI platforms like ChatGPT. In the quick interaction with Amit Singh, he highlights that there is a risk of users' IP addresses and the on-site interactions might be shared with third-party prospects for their business objectives

■ What are the privacy risks ChatGPT poses to users due to its ability to collect personal data?

Generative AI can be complex in terms of privacy, but it also largely depends on the information users put on the internet. For example, OpenAI did state that it crawls millions of websites containing private information to collect training data. Additionally, there is still the matter of contextual integrity, which is the idea that personal information shouldn't be disclosed outside of the initial context in which it was given.

In response to these obvious risks to privacy, regulations such as the European Union's GDPR, Canada's PIPEDA, and California's CCPA have recently introduced policies to help mitigate these concerns. It is becoming increasingly important for all organizations, from startups to larger enterprises, to be aware of these risks as well as the global rules being introduced to respond to them.

■ Is there a possibility of ChatGPT being misused to track users' activities and preferences or being used to commit identity theft or phishing scams?

As ChatGPT is still in its nascent stages, OpenAI's privacy policies are constantly evolving. Recently, OpenAI clarified that it no longer uses the

data submitted through its API for model training. While this is promising, there is still no policy or mechanism as of now that prevents a user from voluntarily opting to provide personal information in the prompts. This is where it gets tricky, as OpenAI would not be able to remove any data once entered. As far as we know, OpenAI does crawl through personal data, but there's no documentation to see how exactly it takes place.

■ What are the security measures offered by ChatGPT? Are they enough to safeguard user privacy and data?

Generative AI as a whole is evolving and is in a nascent stage at present.

There is also the risk that this information might be shared with third-party prospects for their business objectives.

With its growing popularity as the platform to generate responses to user queries, ChatGPT is being used by many of the employees inside their organizational network. What are the implications of its usage in the organizational network and what are the precautions employees need to take to avoid any uncomfortable situation?

All enterprises, from startups to global

disclosure of personal data, and organizations should be prepared to notify the concerned parties in the event of a data breach.

Along with legal compliance, the ethical ramifications of generative AI must be taken into account, and measures must be taken to guarantee that the technology is used in a transparent, accountable, and responsible manner. Also, generative AI models can be audited regularly to make sure they are being utilized properly. This will help build clear standards and procedures for the responsible use of generative AI.

■ How are enterprises and security teams gearing themselves to fight against any unforeseen disaster arising due to ChatGPT in their organization?

It is becoming increasingly important for privacy regulators, legislators, and IT workers to be aware of the privacy risks that generative AI poses. Although generative AI can fundamentally alter how businesses collect and use data, it also comes with substantial privacy threats. To reduce these dangers, it is essential to put privacy safeguards in place, maintain legal compliance, and comprehend the ethical ramifications. By taking these actions, companies can use generative AI tools with the knowledge that they are utilizing innovation safely with the good of society in mind.

“Generative AI as a whole is evolving and is in a nascent stage at present. Privacy regulations are still being worked on, so for the time being, it is the users' responsibility when it comes to the data they put on these platforms.”

Privacy regulations are still being worked on, so for the time being, it is the users' responsibility when it comes to the data they put on these platforms.

Organizations and individuals need to be wary of OpenAI's loopholes in data collection and sharing, including the ones concerning users' IP addresses and the on-site interactions that take place.

corporations, should be concerned about the possible effects that generative AI may have on data privacy. Organizations must ensure that individuals are fully informed about how their data is used and that all data is collected and used with explicit consent. Strong security measures should also be implemented to prevent unauthorized access to or

Micron Technology Inc Forecasts 60% Revenue Drop in Q3, Plans for a Record 2025 with AI Boosting Sales

Discover how Micron Technology Inc. (MU.O) plans to use artificial intelligence to boost sales in 2025. Learn about their headcount reduction, capital investments and how generative AI is fueling the need for storage. Find out about the record calendar year 2025 market size, the two planned factories, and how their revenue and profits have been affected by the chip glut.

Despite an industry-wide chip glut, Micron Technology Inc (MU.O) on Tuesday forecasted that its third-quarter revenue would drop by nearly 60% from the prior year, a figure in line with Wall Street expectations.

Company executives also reported a positive outlook for 2025, citing the growth of artificial intelligence as a sales booster. As part of its strategy to weather the economic downturn, Micron is targeting a 15% reduction in headcount and will keep investments at \$7 billion for the 2023 fiscal year. Matt Bryson, Wedbush Securities chip analyst, praised the firm's decision to lower capital expenses as a move that could "pull forward the timing and breadth of a future recovery".

During the earnings call, Micron President and CEO Sanjay Mehrotra was confident about the memory chip industry's future, predicting a record size for the calendar year 2025. The need for data

centers is also on the rise due to the proliferation of generative AI chatbots, such as Microsoft Corp (MSFT.O)-backed OpenAI's ChatGPT, and this is having a mitigating effect on the demand for chips. The utilization of AI is creating a surge in storage needs, with Chief Business Officer Sumit Sadana noting that a typical AI server requires eight times the amount of DRAM and three times the amount of NAND of a standard server. Micron reported a 53% drop in second-quarter revenue to \$3.69 billion and a net loss of \$2.3 billion, compared to a profit of \$2.26 billion last year.

The company expects to incur a loss of \$1.58 per share in the current quarter, plus or minus 7 cents, which is in line with analyst predictions. The firm also said customer inventories are improving and that it anticipates gradual improvements to the industry's supply-demand balance, as well as improvements to gross margins.

Zscaler Appoints Karl Soderlund as Senior Vice President, Worldwide Partners, and Alliances

Cloud security provider Zscaler has appointed Karl Soderlund as Senior Vice President, Worldwide Partners, and Alliances. His role at Zscaler will involve heading a top-notch channel team and building and implementing a competitive go-to-market strategy in order to advance and modernize the company's partner program.

Dali Rajic, Chief Operational Officer of Zscaler, stated that his company is attracting great personnel since it is the industry leader in cloud security. "Karl is the appropriate industry veteran to take our channel partner program to the next level, as evidenced by his deep partner expertise and track record of successfully implementing highly strategic partner programs at leading networking and cybersecurity organizations I am happy to welcome Karl to the firm and am certain that his efforts will yield results and help company growth as we continue to make significant investments in our partner model."



**KARL SODERLUND, Senior Vice President,
Worldwide Partners, and Alliances, Zscaler**

Leading system integrators, managed service providers, solution providers, and distributors make up the Zscaler partner program, which is constantly adding new partner classes that are uniquely qualified to assist businesses in utilizing the Zscaler Zero Trust Exchange platform. 95 percent of the business for the company is brought in by the partner program. The Zscaler partner program offers broad-based enablement across the lifetime of Zscaler's clients in addition to access.

Soderlund formerly worked as a senior vice president at Palo Alto Networks before joining Zscaler. During the course of his career, Soderlund has received eight channel chief awards, and for the past three years, he has been named one of the top 50 most significant figures in the sector. He also held key positions at Aruba Networks, Avaya, HP, Cisco Systems, and Fortinet before joining Palo Alto Networks.

Salesforce Launches Generative AI for CRM, Einstein GPT



Salesforce has launched generative AI CRM technology Einstein GPT that delivers AI-created content across every sales, service, marketing, commerce, and IT interaction, at a hyper-scale. Salesforce will use generative AI to change every customer experience with Einstein GPT. Salesforce's proprietary AI models will be enhanced by Einstein GPT with real-time data from the Salesforce Data Cloud, which ingests, harmonizes, and integrates all of a company's customer data, as well as generative AI technologies from an ecosystem of partners.

Customers can then use natural language prompts within their Salesforce CRM to generate content using Einstein GPT that continuously adapts to changing customer information and needs in real-time. Customers can connect this data to OpenAI's advanced AI models out of the box or select their own external model.

For instance, Einstein GPT can automatically generate code for developers and generate personalized emails for salespeople

to send to customers. It can also automatically generate targeted content for marketers to improve campaign response rates and specific responses for customer service representatives to answer questions more quickly.

"With the emergence of real-time technology and generative AI, the world is going through one of the most dramatic technological changes. This is significant because every business is working to engage with customers in more intelligent, automated, and personalized ways right now, according to Marc Benioff, CEO, Salesforce. "Einstein GPT is another way we are opening the door to the AI future for all of our clients. We'll be integrating with OpenAI at launch. It works in conjunction with our Data Cloud and is integrated with all of our clouds, as well as Tableau, MuleSoft, and Slack."

Integrating with OpenAI: To produce accurate and dependable AI-generated content, Salesforce is fusing OpenAI's enterprise-grade ChatGPT technology with its own private AI models.

Sam Altman, CEO, OpenAI, said, "We're pleased to apply the power of OpenAI's technology to CRM. This will enable more individuals to take advantage of this technology, and it enables us to learn more about real-world usage, which is essential for the responsible development and deployment of AI, a belief shared by Salesforce and us.

Salesforce Ventures' \$250 million Generative AI Fund is another new initiative the firm has made public. Salesforce Ventures is the company's international investment arm. The new \$250 million fund will support the ecosystem, make investments in high-potential startups, and encourage the creation of creative, trustworthy AI.

Einstein GPT in CRM
The latest version of Salesforce's Einstein AI technology, known as Einstein GPT, will generate more than 200 billion AI-powered predictions every day across Customer 360. Additionally, clients can use ChatGPT or other top large language models in conjunction with proprietary Einstein AI models to combine natural language

prompts with CRM data to activate potent, time-saving automation and produce personalized, AI-generated content. Launching today are:

- **Einstein GPT for Sales:** Automate sales tasks including email creation, meeting scheduling, and interaction planning.
- **Einstein GPT for Service:** Convert case notes from the past into knowledge articles. Create customized agent chat responses automatically to speed up service encounters and improve customer satisfaction.
- **Einstein GPT for Marketing:** Personalized content is generated dynamically to engage clients and prospects across email, mobile, online, and advertising.
- **Einstein GPT for Slack:** Provide AI-powered customer insights via Slack by surfacing end-user behaviors like editing knowledge articles and providing smart summaries of sales prospects.
- **Einstein GPT for Developers:** With Salesforce Research's in-house Big Language Model, increase developer productivity by leveraging an AI conversation assistant to generate code and ask questions for languages like Apex.

Slack ChatGPT, created by OpenAI: Moreover, the ChatGPT for Slack app is being introduced by Salesforce and OpenAI. New AI-powered chat summaries, tools for learning about any subject, and writing support are all provided by this app.

UiPath Integrates Automation Workflows with Amazon SageMaker to Amplify ML Models

Enterprise automation software company UiPath has announced data science teams using Amazon SageMaker, an end-to-end machine learning (ML) service, can now connect to UiPath to seamlessly connect new ML models into business processes without the need for complex coding and manual efforts.

Data scientists, ML developers, and business analysts can easily automate deployment pipelines with the help of the UiPath Business Automation Platform, which lowers the cost of experimentation and speeds up innovation.



ANKUR MEHROTRA,
General Manager, Amazon SageMaker,
AWS

With fully managed infrastructure, tools, and processes, Amazon SageMaker is a completely managed service from Amazon Web Services (AWS) that allows users to prepare data, construct, train, and deploy ML models for any use case. By connecting Amazon SageMaker to UiPath, users can:

- Deploy ML models quickly into production by using UiPath robots to automate workflows and control end-to-end business processes, integrating Amazon SageMaker ML models into automation workflows without writing any code, and connecting freshly finished ML models into production

workflows in minutes.

- Improve the efficiency of data science teams by facilitating precise and consistent procedures that require less human interaction and free up essential resources for strategic work. Organizations can significantly reduce the workload on data science teams by using UiPath automation to roll out the most recent ML models to end users. By reducing human error while keeping human oversight to fulfill governance and compliance criteria, teams can also increase reliability.
- Boost the rate of machine learning innovation by allowing engineering teams to test their theories, take on new tasks, and experiment with their data more regularly. Automation increases the speed and dependability of new model deployment into business processes and eliminates the need for manual script coding, troubleshooting, and maintenance across the whole ML data pipeline.

"With the connection with UiPath, our goal is to assist clients to expedite the deployment of their machine learning models while utilising optimum infrastructure," said Ankur Mehrotra, General Manager, Amazon SageMaker, AWS.

"Data scientists and data science team leaders are at the forefront of machine learning research, developing strong new models to boost company performance." According to Graham Sheldon, Chief Product Officer, UiPath, these specialists are also burdened with time-consuming, manual administration, which delays development and raises costs. "We are using automation to assist decrease this complexity by integrating Amazon SageMaker with the UiPath platform. This creates chances for machine learning innovation through speedier deployment at cheaper prices."

CONVOKE: ALOGIC Strengthens its Partnerships with a Dedicated Partner Meet in Mumbai



ALOGIC recently held a partner meet in Mumbai, named 'CONVOKE', in an effort to build a stronger connection with their partners.

ALOGIC highlighted wide range of products, such as Docking stations, USB-C Hub, Adapters, Converters, Wall Charger, Charging Cable, Stands and Audio-Video cables, and addressed the partners' challenges and queries. Additionally, Mr Suresh Balaji, ALOGIC's country head, was present to address any individual concerns. With the successful execution of the meet, ALOGIC is keen to ensure customers can access the most suitable product according to their requirements when they visit any of its partner shops.

ALOGIC highly values its partners and acknowledges their essential role in helping the brand attain successful growth. The company has dedicated much effort to strengthen its relationships with resellers and systems integrators, and the results of its trade schemes have been well-received. Furthermore, ALOGIC is devoted to solidifying its presence in the minds of its partners. Mr Suresh Balaji, Country Head of ALOGIC Electronics India Pvt Ltd., expressed his enthusiasm for the Mumbai IT market's response to the event.

Redington Partners with Indusface to Strengthen Application Security for Enterprises



Redington has partnered with Indusface, an application security SaaS company, to offer enterprises comprehensive solutions for application security.

The AppTrana platform from Indusface offers a variety of security options to shield web apps from cutting-edge online attacks. A cloud-based web application firewall, DDoS and bot mitigation, a secure content delivery network (CDN), and a threat intelligence engine are some of these options. By their partnership with Indusface, Redington's customers are now able to take advantage of the platform's numerous security features, namely AppTrana, which will enable them to develop effective security plans and defend their apps against changing cyber threats. This relationship is especially important because fraudsters are utilizing more advanced strategies, and businesses need to keep on top of the latest developments to safeguard their

sensitive information and assets.

Rakshit Bhatt, Head Cloud, Business Group, Redington, stated that cyber security is a crucial aspect of digital transformation and that Redington is dedicated to providing our customers with the best-in-class solutions to secure their digital assets. "We are thrilled to collaborate with Indusface, who has a lot of application security knowledge and expertise. By this agreement, we will be able to provide our clients with robust and all-encompassing security solutions that will strengthen their resistance to modern threats."

A recent Indusface study found that by employing custom rules, approximately 60% of attacks were stopped. The benefit that Indusface offers is the capacity to function as an extended SOC team to create, test, and maintain bespoke rules while guaranteeing a zero false positive rate. The core rules are comparable to those of other WAAP providers.

Tech Mahindra Appoints Mohit Joshi as MD & CEO Designate, Poised to Take Over in 2023

Tech Mahindra announces Mohit Joshi as its new MD & CEO designate, who will take over from current MD & CEO CP Gurnani in December 2023.

The Board of Tech Mahindra, a leading provider of digital transformation, consulting and business re-engineering services and solutions, today announced Mohit Joshi as the MD & CEO designate. He will assume the position of MD & CEO upon CP Gurnani's retirement on 19th December 2023, and will be joining the company beforehand to facilitate a seamless transition.

Having previously worked at Infosys, where he was President of the company, Mohit brings



MOHIT JOSHI,
MD & CEO Designate, Tech Mahindra

over two decades of experience in the Enterprise technology software & consulting field and has been instrumental in the digital transformation of some of the world's largest companies. At Infosys, he was Head of Global Financial Services & Healthcare and Software businesses, which included Finacle (the banking platform) and the AI/Automation portfolio, as well as Sales Operations, Transformations, large deals and the CIO function.

Volante Technologies and HCLTech Forge Strategic Alliance to Unlock Financial Innovation



Volante Technologies, a premier global supplier of cloud payments and financial messaging solutions, has entered into a strategic partnership with HCLTech, a leading worldwide technology enterprise. The firms will collaborate to promote payments modernisation, assisting financial organisations to keep up with the fast-paced digital revolution taking place in the industry.

HCLTech will be combining its digital and engineering services expertise with Volante's cloud-native payments solutions and low-code financial platform, allowing financial institutions to rapidly deploy solutions for immediate payments, real-time gross settlement (RTGS) payments and domestic and international payment methods. The organisations are also dedicated to developing centers of excellence in India and Romania to support the configuration, customisation, integration and execution of Volante's ecosystem of business services for payments modernisation.

Srinivasan Seshadri, Chief Growth Officer and Global Head of Financial Services at HCLTech, commented that the collaboration with Volante will enable their customers to operate in a stable, scaleable and adaptable payments environment and improve the time-to-market speed. Jim Chow, Vice President for Partnerships and Business Development at Volante Technologies, expressed that their partnership with HCLTech was extremely promising and that their shared vision of payments would be available to a wider range of customers and financial services organisations. Deepak Gupta, Senior Vice President & Global Head of Payments as a Service and Strategic Partnerships for Volante Technologies, added that the joint centers of excellence would allow them to expand their international presence faster and have access to local know-how and engineering capacities.

At present, HCLTech and Volante Technologies are engaged in multiple implementation projects with some of the largest banks in the world.

ManageEngine Unveils Security & Risk Posture Management Dashboard for Comprehensive SIEM Solution.

ManageEngine, the enterprise IT management arm of Zoho Corporation, has unveiled a security and risk posture management dashboard for Log360, its comprehensive SIEM solution with built-in DLP and CASB tools. Through this feature, enterprises have the ability to formulate proactive security tactics and avert potential cyberattacks. To effectively create a proactive security strategy, organizations must gauge their network risks regularly. Risk evaluation and management, when conducted properly, can reinforce the security of their networks and thwart cyber criminals from infiltrating their infrastructure. Regulatory requirements across regions necessitate enterprises of all sizes and sectors to abide by security protocols to bolster their network systems. Active Directory (AD) is usually a top target for cyber criminals. Evaluating AD risks constantly and ameliorating its security posture are imperative for avoiding potential cyberattacks.

Preventing unauthorized access to sensitive data requires an organization to harden their Active Directory (AD) security. Log360's Security and Risk Posture Management allows organizations to proactively protect against security threats by preempting intrusions. This strategy is essential to comply with various regional compliance mandates and is an increasingly frequent topic in board meetings. Manikandan Thangaraj, vice president of ManageEngine, explains the importance of this proactive security measure.

Log360 provides extensive machine learning-based user and entity behavior analytics, allowing it to actively monitor user behavior and detect potential identity theft. With the combination of all these features, Log360 offers comprehensive protection against account compromise and identity theft, as well as facilitating rapid response to potential security breaches.

Linksys and Fortinet Announce Strategic Alliance to Deliver Enterprise-Grade Performance and Security for Work From Home Networks

Fortinet Invests \$75M in Linksys to Support Alliance to Offer Organizations Fast, Reliable, Secure, and Simple to Manage Remote Connectivity



Ken Xie

Founder, Chairman of the Board, and CEO at Fortinet



"When organizations implement telework at scale, cyber criminals leap at the opportunity to exploit the numerous security gaps that arise. Security-driven networking—a strategy that converges networking and security across the connected environment, from the core,

into the cloud, and to the branch and remote workers—enables organizations to see and defend today's highly dynamic environments while preserving an excellent user experience. We are excited to partner with Linksys to deliver enterprise-grade secure, reliable network connectivity for home-based workers."

Sidney Lu,

Chairman and CEO of FIT Hon Teng



"We are pleased to welcome Fortinet as a strategic partner in providing secured connectivity for consumers and remote professionals. The collaboration is a testament to the ongoing strength and reach of the Linksys business. We look forward to leveraging Fortinet's proven cybersecurity expertise to capitalize on new opportunities."

News Summary

Linksys, a global leader in wireless networking products, a subsidiary of Foxconn Interconnect Technology (6088.HK) ("FIT") and Fortinet (NASDAQ: FTNT), a global leader in broad, integrated and automated cybersecurity solutions, today announced a strategic alliance with the

intent to further secure and optimize the performance and management of home networks in today's work from home environment.

Together, Fortinet, Linksys, and FIT will offer enterprise-grade connectivity and security and unparalleled quality of service to organizations that need to provide seamless and secure connectivity for their employees to efficiently work from home.

As part of the alliance, Fortinet has made a strategic investment of \$75M in Linksys, which provides leading and next-generation router connectivity solutions to consumers and businesses worldwide. In addition, Fortinet will appoint a representative to the Linksys Board of Directors.

UBS-Credit Suisse Merger and US Banking Troubles to Impact India's IT BPM Industry



This month, the US witnessed banking troubles with Silicon Valley Bank (SVB) and Signature Bank being taken over by the Federal Insurance Deposit Council (FDIC). In response, European regulators brokered a deal for banking giant UBS to acquire crisis-stricken Credit Suisse, one of the largest banking mergers and acquisitions in the region.

Moody's has put First Republic, Western Alliance Bancorp., Intrust Financial Corp., UMB Financial Corp., Zions Bancorp. and Comerica Inc. under review for potential downgrades due to concerns about potential losses in asset portfolios.

Warnings from analysts

suggest that the banking crisis in the US and Europe could have a detrimental impact on India's \$245 billion IT BPM industry, which is reliant on the BFSI sector for 41% of its income. The collapse of major banking institutions could result in decreased business and deferred payments. Analysts suggest that if large banking institutions collapse, it could lead to a decrease in business and deferred tech investments in the future, as well as delayed financial transactions. Companies such as TCS, Infosys, Wipro, and Mindtree, which largely depend on US banking institutions, may be impacted if the crisis worsens. A JP Morgan's report last week showed that the exposure of regional US banks to the two largest

Indian IT companies, TCS and Infosys, is 2-3% of their total revenue.

Celent, a financial advisory firm, reported that North American banks are the biggest contributors to tech investments in retail banking worldwide, with an estimated budget of \$82 billion out of the global expenditure of \$250 billion in 2022. Indian IT companies have benefited significantly from the BFSI's (Banking, Financial Services, and Insurance) tech spending.

Nasscom estimates that the Business Financial Services (BFSI) industry contributes approximately 41% of total enterprise technology expenditure in FY23. North America accounts for more than

half of the revenue for companies in this sector, with Wipro topping the list at 35%, followed by TCS (31.5%), Infosys (29.3%) and HCLTech (20%). Tech Mahindra has the lowest share of the sector among the top IT firms, at 16%. It is estimated that the SVB exposure of TCS, Infosys and LTIM could lead to provisions in the last quarter of FY2023.

The macroeconomic environment could also reduce short-term technology investments by banks, leading to slower growth of bank technology budgets. This could cause delays in project ramp-ups and deal closures that could affect revenue over the next three to four quarters.



Tech for a Sustainable Future

Sustainability has moved swiftly up the executive agenda in recent years. Even at the height of the Covid-19 pandemic, becoming a truly sustainable and responsible business was a top priority for most CEOs.

Beyond the great promise of protecting people and the planet, companies with a higher sustainability performance—across environmental, social, and governance (ESG) indicators—perform better financially than their peers.

Just as digital transformation required every company to become a technology company, with technology at its heart, now every business needs to become sustainable—and technology is again taking center stage.

Technology is—and will continue to be—the fundamental driver of sustainability for organizations, and their supply chains, customers, and broader business ecosystems. As per a recent Accenture survey, 92% of companies aim to achieve net-zero targets by 2030, which will require the deployment of advanced technologies to measure, reduce, and remove an organization's carbon footprint. Technology is essential to improving transparency and traceability in global supply chains. It helps companies uncover insights to spur action, whether that means transforming customer experiences or building a more sustainable organization.

While technology is a fundamental driver of sustainability, the solution itself needs to be monitored so that it doesn't become a problem. Technology can and does create sustainability issues. For example, training a single AI model can emit as much CO₂ as five relatively ordinary cars do in their lifetimes. And using a mobile phone for just one hour a day for one year produces some 1.4 tons of CO₂—that's more carbon emissions than two round-trip flights between London and Glasgow. This brings technology within the ambit of the sustainability efforts of organizations. Hence, the priority must be to design and deploy sustainable, green technology to harness the benefits of meeting the sustainability agenda.

There are clear benefits to harnessing technology to drive sustainability. In fact, companies that adopt sustainable technology to a significant extent achieve 4% higher ESG scores on the Arabesque S-Ray dataset—a global specialist in measuring ESG metrics—than those that do not. This can translate into an 11% jump in their ESG ranking. And between 2013 and 2020, companies with consistently high ESG performance tended to generate 2.6-times higher total shareholder returns, compared to those with mid-range ESG scores.

So, what's holding back organizations? For many, the transformation is daunting. Nearly one-fifth of the organizations say their biggest challenge is that they are not aware of the unintended consequences of technology. Lack of ready solutions is a big concern, as is the complexity associated with adopting these solutions. And then, there's what we call the intent-action gap—only 7% of companies have fully integrated their business, technology, and sustainability strategies.

As sustainability strategies take shape, the IT Leader of the business will be the common denominator as different members of the C-suite take "ownership" of specific aspects and become reliant on technology to achieve their objectives.

Moving ahead, CXOs must take a fresh look at their technology through the lens of sustainability. In this issue of ITPV Magazine, we have highlighted comprehensive sustainable technology strategy—one that makes technology more sustainable and uses that technology to drive sustainability at scale. It is time to push the reset button and reimagine a healthier, wiser, and sustainable world!

Enjoy reading and please don't forget to share your feedback at kalpana@techplusmedia.co.in

Kalpana Singhal

KALPANA SINGHAL, Editor
(E-mail: kalpana@techplusmedia.co.in)

EDITOR: KALPANA SINGHAL
CONTENT HEAD: Amit Singh
ASSISTANT EDITOR: Rajneesh De
CORRESPONDENT: Aaratrika Talukdar
CORRESPONDENT: Atreyee Chakraborty

INTEGRATED MARKETING COMMUNICATION:

Aakash Vahal
Saugata Mukherjee, Mamta Dhiman,
Nishit Saxena

ASSOCIATE ANALYST
Shaithra S

SALES:
Harpreet Singh | Pratap Jana

PRODUCTION HEAD:
Aji Kumar

WEBSITE:
Sheetal Varshney/Ramesh Kr

PROMOTION:
Vikas Yadav /Amit Pandey

CIRCULATION:
Pratap

FINANCE:
Inder Pal

HEAD OFFICE:
370A, Sant Nagar, East of Kailash, New Delhi
Tel: 41625763, 26237405, 41620042
Email - kalpana@techplusmedia.co.in

MARKETING OFFICE:
10 UF, West Wing, Raheja Tower,
MG Road, Shanthala Nagar, Ashok Nagar,
Bengaluru, Karnataka-560001

Delhi: 9711841991 | **Mumbai:** 9711841992
Kolkata / Guwahati: 9331072026
Bangalore: 9354347953

OWNED, PRINTED & PUBLISHED BY ANUJ SINGHAL Printed at Modest Graphics Pvt. Ltd., C 52-53, DDA Shed, Okhla Industrial Area, Phase - I, New Delhi-20, Place of Publication: 370A, 2nd Floor, Sant Nagar, East of Kailash, New Delhi-110065, Editor- Anuj Singhal

ITPV does not claim any responsibility to return adequate postage. All rights reserved. No part of this publication may be reproduced in any form without prior written permission from the editor. Back Page AD will carry RNI Number & Imprint Line

Note: While every possible care is taken prior to accepting advertising material, it is not possible to verify its contents. ITPV will not be held responsible for such contents, or for any loss or damages incurred as a result of transactions advertising/advertisement in this publication. We recommend that the readers make necessary inquiries and verification before remitting money or entering into any agreement with advertisers, or otherwise acting on advertisement in any manner whatsoever.

#1 Backup for Service Providers

Exceed Customers Service level
agreements (SLAs) while increasing
margins & revenue

PANTUM
प्रिंटिंग के लिए नया युग

Pantum India Product Line

Business is Complicated, Printing Should be Simple

Vibrant 18 Series



Elite Series



PT-L280 Series



PT-L380 Series



PT-B680 Series



Simple&Smart Series



Simple&Smart Series



Mighty Series



4S Efficiency Series



Max Series

PANTUM SERVICE TOLL FREE NO.: 18003098240

WWW.PANTUM.IN

SALES REGION	PHONE NOS.	SALES REGION	PHONE NOS.
West Bengal & North East	98302 28532	Bihar & Jharkhand	9334317035

Know more on @PantumIndia