BPO industry leads agentic AI adoption in PHL

By Almira Louise S. Martinez
Reporter

THE BUSINESS process outsourcing (BPO) industry is leading the adoption of agentic artificial intelligence (AI) in the Philippines as companies transition from experimentation to application of AI solutions, the International Business Machines Corp. (IBM) said.

"In the Philippines, we have seen in the BPOs a lot of AI usage in call centers in terms of intent analysis or conversation summarizations," IBM APAC Head of Client Engineering Anup Kumar told *BusinessWorld* in a virtual interview.

"I will say they are the leaders for sure. They are the ones who have the necessary means to move forward with the piece."

Agentic AI uses "agents" for specific tasks with minimal human supervision. These systems can work autonomously and make decisions based on data, probability, and patterns learned from interactions.

Unlike traditional AI models, which still require human intervention, agentic AI exhibits "autonomy, goal-driven behavior, and adaptability," IBM said.

"It started from typical machine learning, to becoming like an AI assistant, to now a bit of an autonomous agent or assistant," Mr. Kumar said.

While many industries are already using agentic AI solutions in their operations, some sectors find it harder to tap these technologies, he said.

"I think the biggest challenge at the moment is the organizational challenge itself," Mr. Kumar said. "An organization has to start thinking about how the agent will help and also how to start trusting it."

The cost of deploying agentic AI is another hurdle, he added.

"A lot of the way people are building it is through LLMs (large language models) hosted on cloud providers, and the bigger you're using, the bigger it costs. So, that is also preventing a lot of customers from going mainstream."

As agentic AI continues to evolve, organizations need to be able to adapt so that they can leverage the potential of these technologies, he said.

"While I will say that some part of agentic AI, like in terms of workflow automation by using tools, is doing multiple agent orchestration, I will say there's a need for a bit more maturity in terms of the technology," he added.

In 2024, the BPO industry employed around 1.4 million in the Philippines. It has also generated about $38 billion in revenue, making it a vital part of the country's economy.

The 2025 Work Trend Index report by Microsoft revealed that 60% of Philippine leaders are extremely familiar with AI agents, while only 42% of employees are familiar with the technology.

It added that about 89% of Philippine leaders said they are confident about having AI agents as digital team members to expand their workforce capacity in the next 12 to 18 months.

Cybersecurity needs a rethink in the age of agentic artificial intelligence

By Asha Hemrajani

OPINION

ARTIFICIAL INTELLIGENCE (AI) has entered a new phase. It is shifting from passive tools to autonomous agents that can plan and act across digital and physical systems, often for extended periods and in concert with other agents. Their interacting and collaborating capabilities are scaling quickly, allowing them to perform increasingly complex tasks with minimal human input, across sectors such as banking, e-commerce, and logistics.

These systems are improving efficiency, but they also raise the stakes for cybersecurity as many of them were not built with security in mind.

Agentic AI systems can be attacked. As they interact with enterprise systems, other agents, and humans, the cybersecurity attack surface expands, exposing them to new threats such as impersonation attacks, prompt injections and data exfiltration.

The boundaries between appropriate autonomous use and deliberate misuse are blurring as enterprises permit AI agents to use apps on users' behalf more frequently. Malicious agents can also take advantage of the same interfaces that authentic agents employ.

Safeguarding agentic AI in enterprise systems is therefore emerging as one of the defining upcoming cybersecurity challenges.

Recent state-linked campaigns such as UNC3886, reported in Singapore, revealed how adversaries try to exploit trusted enterprise platforms to gain persistent access. Similar risks will arise as agentic systems become more deeply integrated into operations. Protecting them is no longer optional; it is a strategic imperative.

CYBERSECURITY AS A STRATEGIC ENABLER

Traditional cybersecurity frameworks were designed for systems with predictable behaviors. Agentic AI breaks that predictability. It learns, adapts, and operates with varying degrees of autonomy, creating new layers of uncertainty that static defenses cannot contain.

For governments and large enterprises operating critical infrastructure, this shift requires a fundamental change in mindset. As agentic AI becomes embedded in decision-making, operations, and citizen services, cybersecurity must evolve from a defensive function to a strategic enabler of trusted autonomy.

Purposeful and appropriate agentic AI deployment is critical. The right safeguards are needed for such deployments. Deeper testing of how AI systems interact, along with clear human oversight and escalation management is essential, especially in critical infrastructure.

Security must now be adaptive, context aware, and integrated into business and operational strategy. It is no longer just about preventing attacks. It is about maintaining the trustworthiness of autonomous systems that are starting to influence decisions at national and enterprise scale.

The distinction between securing AI deployment and leveraging AI in cybersecurity is also one that needs to be recognized. Guardrails for this nascent field are still in a formative phase, but ethical and practical implementation realities are important pieces of the puzzle that cannot be ignored.

Fundamental signposts in cybersecurity also need revisits and rethinks. Identity, data and attack surfaces take on different complexions that are still evolving, and there are contradictory philosophies in concepts such as Zero Trust that need adaptation to the growing impact of AI.

REFRAMING DIGITAL RISK GOVERNANCE

Governance frameworks must evolve alongside technology. Two issues are becoming urgent.

First, the spectrum of autonomy must be understood. Agentic behavior is not a binary state. Treating a basic automation script as equivalent to a self-directing system results in misplaced controls and uneven risk management. Oversight and safeguards should correspond to degrees of autonomy, not broad labels.

Second, accountability must be redefined. If an agentic AI system executes an action that is harmful, who should bear responsibility? Without clear boundaries, legal and ethical gaps will persist, and adversaries may exploit them. Boards, chief information security officers, and regulators need shared accountability models that reflect how agentic AI systems work.

These questions are already visible in data governance disputes, algorithmic bias cases, and AI incidents where AI systems have behaved in unexpected ways. Unless accountability frameworks get better defined, accountability gaps will widen.

SECURING AGENTIC AI IN CRITICAL INFRASTRUCTURE

Agentic AI deployment in critical infrastructure entities raises unique risks. Agentic AI promises gains in efficiency and resilience, but its vulnerabilities could cause cascading disruptions if compromised.

Protecting these systems requires new approaches to securing AI apps and agents.

It is essential that critical infrastructure entities retain control as they adopt more autonomous AI-driven systems.

Hence, the focus needs to be on detection and stopping attacks (such as direct and indirect prompt injection, data poisoning) on models/AI apps and agentic-AI workflows. Policy control for AI use such as blocking risky requests, data-leak prevention for AI apps, and detecting unsanctioned AI agents in use, among others, are also essential.

Equally important is ensuring resilience in agentic AI systems by governing the non-human identities (NHIs), the digital identities backbone of agentic AI. Enterprises will need to exercise proper oversight of NHIs in terms of access control, guardrails, and traceability.

CONVENING FOR RESILIENCE IN AGENTIC AI

No single government, enterprise, or regulator can address these challenges on their own. For agentic AI systems to be safe and resilient, collaboration across borders and sectors is needed.

Across ASEAN, economies like Singapore, Malaysia, and the Philippines are building stronger partnerships between government, industry, and academia to prepare for the next wave of AI-driven threats. Platforms such as GovWare in Singapore play an important role in connecting regional voices and advancing dialogue on shared cybersecurity challenges that affect the entire ASEAN digital ecosystem.

The real value of such forums lies in bringing together policymakers, enterprises and innovators to address accountability, interoperability and resilience together.

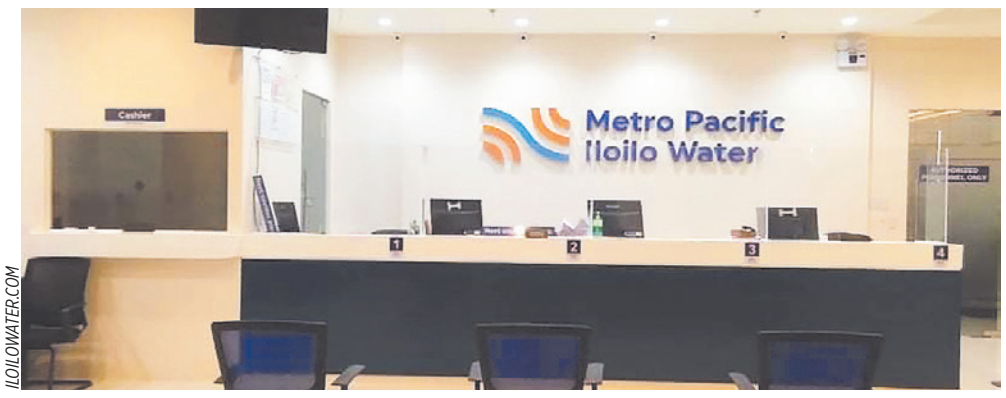
BUILDING TRUST IN THE AGE OF AUTONOMY

As agentic AI becomes part of daily operations, the real challenge is not only technical but human. Trust will depend on the people who design, deploy, and oversee these systems, and on their ability to step in when things go wrong.

Events like GovWare help translate complex AI and cybersecurity issues into shared understanding and practical collaboration. They remind us that resilience is built through people working together, not machines acting alone.

Ultimately, technology is only as trustworthy as the intent and integrity of those who create and use it. A secure digital future will depend on our collective willingness to stay curious, accountable, and connected, because trust is built by people, not algorithms.

ASHA HEMRAJANI is the senior fellow at the S. Rajaratnam School of International Studies at Nanyang Technological University, and Ian Monteiro, CEO and founder of Image Engine.



ILOILOWATER.COM

MPIW defends tariff adjustment, says increase to sustain operations

METRO PACIFIC Iloilo Water (MPIW) said the recent tariff increase approved by regulators is necessary to sustain its water distribution operations in Iloilo City amid rising costs.

"This tariff adjustment does not fund infrastructure projects or capital expenditures," MPIW Commercial Department Head Kathleen Sadio said in a media release on Wednesday.

"It ensures we can continue operating efficiently, meeting regulatory standards, and delivering consistent service even as inflation, energy costs, bulk water supply costs, and operational demands increase," she added.

The Local Water Utilities Administration (LWUA), which oversees more than 500 water districts nationwide, approved the tariff adjustment that raised MPIW's basic charge to P28.67 per cubic meter (cu.m.) from P20 per cu.m.

MPIW said the increase is "vital to support operational expenses such as power, chemicals, labor, and fuel," emphasizing that it will not be used for capital expenditures.

Ms. Sadio said the company has been subsidizing bulk water supply costs in recent years, prompting the adjustment.

Despite the higher rates, the company said its tariffs remain among the lowest in Metro Iloilo and compared with other highly urbanized cities.

MPIW said it has invested P4.2 billion in water-related projects since taking over operations in 2019.

"We've been operating at a loss for six years, but we're not backing down," Ms. Sadio said. "Even in the face of continuously rising bulk water supply costs, operational and material costs, and regulatory issues, we've made significant progress — because this is our commitment to Iloilo."

The company plans to invest P11 billion over the next five to ten years, including the ongoing P5-billion desalination facility project in Iloilo.

MPIW said project implementation has faced challenges such as coordination with regulatory agencies, supply chain issues, weather disruptions, and permitting delays.

"We've refined some of our processes to be more coordinated and responsive to on-the-ground realities," Ms. Sadio said. "We now implement phased construction, strengthen collaboration with the Department of Public Works and Highways and local government units, and intensify our public communication to minimize disruption."

The company aims to reduce its non-revenue water (NRW) level — or treated water lost through leaks, pilferage, or outdated pipelines — to 35% by 2027.

MPIW is a joint venture between Metro Iloilo Water District and Metro Pacific Water (MPW) that provides water services to Iloilo City and the municipalities of Oton, Sta. Barbara, Cabatuan, Maasin, San Miguel, Pavia, and Leganes.

MPW is the water infrastructure investments subsidiary of Pangilinan-led conglomerate Metro Pacific Investments Corp. (MPIC).

MPIC is one of the three key Philippine units of Hong Kong-based First Pacific Co. Ltd., the others being Philex Mining Corp. and PLDT Inc. Hastings Holdings, Inc., a unit of PLDT Beneficial Trust Fund subsidiary MediaQuest Holdings, Inc., has a majority share in *BusinessWorld* through the Philippine Star Group, which it controls. — **Sheldeen Joy Talavera**