PPP eyed for Mindanao rail after China pullout

By Ashley Erika O. Jose
Reporter

THE Department of Transportation (DoTr) is considering enlisting the private sector for the Mindanao railway project as the government scrambles to put together funding after China bowed out of the project.

"We are also reviewing the feasibility study and the alignment of the rail line. We are talking to many (possible sources of funding) but we are not at liberty to divulge their identity yet. We need to do this project; that is why we are looking for other sources of funds. In fact, this project is also a possible PPP (Public-Private Partnership)," Transportation Secretary Jaime J. Bautista told reporters on the sidelines of the Transport Con 2024 last week.

Mr. Bautista said the government is still considering official development assistance (ODA) for the project, but it is now leaning towards a PPP arrangement.

"We are still open for ODA but if there's PPP we will do that," he said, noting the potential for private partners to move faster. He added that the DoTr is drafting the terms of reference for possible PPP.

The Philippines' dropped China as funding source for the Mindanao Railway project and two more railway projects such as the South Long-Haul railway, and the Subic-Clark Railway project, due to lack of progress on a financing decision in Beijing.

Earlier this year, the Transportation department said that it is finalizing the feasibility study to overhaul the Mindanao Railway's original study to make it more modern and environment-friendly.

"The feasibility study is ongoing now. We are not in a hurry, we need investor confidence. Investors need to know that their investments will be profitable and have a reasonable rate of return," Mr. Bautista said.

"Government should be reminded that the Mindanao railway project is first and foremost a massive development undertaking, which seeks to improve regional economic outcomes and reduce poverty in the countryside," Terry L. Ridon, a public investment analyst and convenor of think-tank InfraWatch PH, said in a Viber message.

Mr. Ridon said the objectives of the Mindanao railway project typically require ODA funding as the commercial case for these projects is not enticing to the private sector.

"In order for the government to have actual proponents, it should first make the commercial case as to why the private sector should take on the Mindanao railway project," Mr. Ridon said.

Nigel Paul C. Villarete, senior adviser on PPP at the technical advisory group Libra Konsult, Inc., said the government needs to assess and understand the private sector's appetite for PPPs.

"Private proponents are after financial returns and they won't enter into anything which is not profitable," Mr. Villarete said.

The viability of adopting a PPP scheme for this project would depend on the project's profitability and economic viability, he added.

Rene S. Santiago, former president of the Transportation Science Society of the Philippines, said PPP would be a solid option for railway projects, especially the operations and maintenance components.

"But it won't address the fundamental deficiencies of the Mindanao railway: it is neither economically or financially viable. To be acceptable for PPP, huge subsidies in construction and operations are needed," Mr. Santiago said.

Libra Konsult's Mr. Villarete said if the government is really leaning towards PPP for a project as massive as the Mindanao Railway, then the government should offer it as a solicited project.

"A railway requires right-of-way (RoW) over its entire length and stations will involve hundreds of small lots along its route," he said.

"The possibility of delays due to RoW acquisition is much higher; these are responsibilities that can only be taken on by the government. Thus, it's better that government to tender this in solicited mode, rather than wait for the private sector to submit proposals, which will entail substantial negotiation on RoW acquisition responsibilities later," Mr. Villarete said.

The first phase of the Mindanao Railway project is valued at P83 billion. It will run from Tagum, Davao del Norte to Digos City, Davao del Sur. It is expected to carry 122,000 passengers per day and cut travel time between Tagum and Digos from three hours to one.

Constraints on PHL consumption growth seen loosened as inflation, rates recede

HOUSEHOLD consumption in the Philippines will rebound due to easing inflation and loosening monetary policy, Bank of America (BofA) Global Research said.

"Consumption growth in the Philippines has lagged overall growth in domestic product (GDP) due to elevated inflation, unemployment, and lagging wages," it said in a report.

"However, these issues are slowly easing, and we think consumption growth has bottomed as inflation recedes, wages and employment catch up."

The economy grew 5.2% in the third quarter, the weakest level in five quarters or since the 4.3% expansion in the second quarter of 2023.

However, household consumption rose 5.1%, improving from 4.7% in the second quarter. Consumption accounts for over 70% of the economy.

"Consumption is most sensitive to income, employment, consumer confidence, and remittances from overseas. Its growth has also been occasionally boosted by tax cuts (2023) and mandated wage adjustments (2022, 2023 and 2024)," the bank said.

BofA expects Philippine GDP to "stay shy" of 6% for this year and the next, below the government's 6-7% and 6.5-7.5% targets, respectively.

However, it sees stronger private consumption at 5.5% for the fourth quarter. It estimates household spending to accelerate to 5.4% in 2025 from 5% this year.

"Some of the anticipated consumption growth drivers have already begun to take root in the third quarter, starting with a sharp slowdown in inflation."

Headline inflation picked up to 2.3% in October, bringing the 10-month average to 3.3%. This was still within the central bank's 2-4% target range.

The Bangko Sentral ng Pilipinas (BSP) expects inflation to settle at 3.1% this year, 3.2% in 2025 and 3.4% in 2026.

Inflation is also expected to ease further after an executive order slashed tariffs on rice imports to 15%, which took effect in July.

"The government also stepped in in the third quarter to cut tariffs on rice imports — the effects of which should be apparent on domestic rice prices by the first quarter of 2025, during which we expect inflation to bottom out."

The Philippine Statistics Authority reported that the average price of regular-milled rice dropped to P50.22 per kilo in October from P50.47 in September, while well-milled rice declined to P55.28 per kilo from P55.51.

"The decline of inflation is also expected to be accompanied by easing monetary policy," BofA said.

BofA expects the BSP to cut rates by a total of 75 basis points (bps) this year. This would bring the policy rate to 5.75% by year's end.

This year so far, the central bank has reduced interest rates by a total of 50 bps since August, when the BSP kicked off its easing cycle.

The Monetary Board has scheduled its last rate-setting review for the year for Dec. 19.

BSP Governor Eli M. Remolona, Jr. has said it is possible to deliver a 25-bp rate cut at the meeting.

BofA also forecasts four 25 bps worth of cuts next year, "roughly at a quarterly pace."

"Unclear if the rate path of the BSP will inflect should the election outcome in the US eventually result in a much stronger dollar as to ultimately alter the domestic inflation outlook," it added.

In a separate report, BofA noted that the Philippine central bank will "ease policy rates in a gradual but consistent manner in the next few quarters, broadly following the Fed."

It also noted that the inflation outlook gives the country "ample space" to continue lowering policy rates.

"For the Philippines, the focus is more exclusively on inflation, which will dictate pace and quantum of rate cuts, while keeping an eye on the exchange rate. BSP could complement rate cuts with RRR cuts," it added.

The BSP reduced the reserve requirement ratio (RRR) for universal and commercial banks and nonbank financial institutions with quasi-banking functions by 250 bps to 7% from 9.5%, effective on Oct. 25.

Mr. Remolona has said the RRR could be brought down to as low as zero before his term ends in 2029. — **Luisa Maria Jacinta C. Jocson**

Sugar industry expects adequate supply despite import freeze until 2025

SUGAR producers said the supply of refined and raw sugar will be sufficient even after the government announced an import freeze until the middle of 2025.

"We do have sufficient supply of sugar — raw and refined — despite the drop in production," United Sugar Producers Federation of the Philippines President Manuel R. Lamata said via Viber.

Last week, the Department of Agriculture and the Sugar Regulatory Administration (SRA) said they intend to postpone refined sugar imports.

The SRA has said that raw sugar production during the current crop year would decline by 7.2% from a year earlier due to crop damage sustained during the dry conditions brought about by El Niño.

Mr. Lamata added he sees the need to import sugar by October 2025.

The Sugar Council and the National Congress of Unions in the Sugar Industry of the Philippines have noted however that mill gate prices for raw sugar have declined.

"An apparent decrease in demand has consequently caused the steady drop in prices," the groups said in a joint statement.

They added that a considerable amount of raw sugar is being withdrawn for refining, despite the stable supply of refined sugar.

"It makes no business sense for refineries to withdraw raw sugar. Hence, demand for it goes down and mill gate prices drop," they added.

According to the SRA, raw sugar stocks hit 148,255 metric tons (MT), while those of refined sugar amounted to 323,923 MT as of Oct. 20.

The Sugar Council said that the drop in demand may have also been due to the increasing use of artificial sweeteners by the beverage industry.

Earlier, SRA said that it would look into the actual volumes of other sweeteners and, if warranted, require them to obtain clearances as well.

In September, the regulator had raised the clearance fee for High Fructose Corn Syrup to P30 per equivalent bag of sugar from P1.5 per bag.

Under tariff code 17.02 of the ASEAN Harmonized Tariff Nomenclature, only high fructose corn syrup is regulated. Artificial sweeteners are admitted at zero tariff under the ASEAN Trade in Goods Agreement. — **Adrian H. Halili**

OPINION

Harnessing the human element in cybersecurity

IN BRIEF:

- Recognizing employees as the cornerstone of cybersecurity, organizations must shift from tech-centric defenses to fostering a vigilant, security-aware culture.
- Comprehensive education and behavioral change strategies are essential to mitigate human-related security risks and reinforce a collective approach to cybersecurity.
- A balanced strategy that combines technological tools with human oversight and continuous cultural development is key to maintaining a resilient cybersecurity posture.

SUITS THE C-SUITE
JOSEPH IAN M. CANLAS
and
CHRISTIANE JOYMIEL C. SAY-MENDOZA

Empowering employees with knowledge and vigilance is as crucial as technology in building a resilient cybersecurity defense.

Cybersecurity threats are more sophisticated and pervasive than ever. While companies invest heavily in advanced technology and security protocols, the most critical line of defense consists of their own employees. Despite having robust security measures in place, organizations frequently find themselves vulnerable due to human error, negligence, or a lack of awareness. This reality underscores the urgent need for a shift in focus — from solely relying on technology to cultivating a culture where every employee actively contributes to cybersecurity.

THE CRITICAL ROLE OF HUMAN BEHAVIOR

The prevalence of cyberthreats in our interconnected world is undeniable, and the assumption that technology alone can safeguard information security and privacy is a misconception. A security-conscious culture within an organization is essential to effectively complement and enhance the technical safeguards already in place.

IT risk management, therefore, must be a holistic practice that not only includes technological solutions but also addresses the human factors that significantly influence the security landscape.

HUMAN ERROR AND SECURITY BREACHES

Human error continues to be a significant contributor to security breaches, with recent statistics from the 2024 Verizon Data Breach Investigations Report indicating that 68% of breaches involve some form of non-malicious human element. According to IBM, the financial repercussions are staggering, with the global average cost of each data breach in 2024 reaching $4.88 million — the highest total ever recorded. This figure reflects direct financial losses and encompasses the long-term reputational damage that organizations suffer following a breach.

Case studies from various industries have shown that breaches often stem from a lack of awareness or negligence, underscoring the importance of addressing human error as a critical component of cybersecurity strategies.

HUMAN BEHAVIOR IN CYBERSECURITY

Delving into the psychological and behavioral aspects of cybersecurity reveals that human actions are often the weakest link in security chains. Common risky behaviors such as password reuse, oversharing on social media, and susceptibility to phishing and social engineering attacks can significantly compromise an organization's security. To effectively mitigate these risks, it is imperative to understand the underlying motivations and cognitive biases that drive such behaviors and to develop targeted strategies that promote secure practices.

To combat the risks associated with human behavior, organizations must implement comprehensive and continuous education programs that raise awareness about the dangers of insecure practices and actively engage employees in adopting and maintaining secure habits. These programs should be dynamic, incorporating real-life scenarios and practical exercises that resonate with employees and foster a sense of personal responsibility for cybersecurity.

SECURITY-CONSCIOUS CULTURE

Creating a security-conscious culture within an organization begins with the development of engaging and effective training programs. These programs should be designed to capture the attention of employees, providing them with the knowledge and skills necessary to recognize and respond to cybersecurity threats. Leadership commitment is crucial in reinforcing the importance of these programs, ensuring that security awareness is not just a one-time event but an ongoing priority.

A human-centered approach to designing security processes and IT risk management is essential. By considering the user experience and incorporating principles of secure-by-design and human-centered design, organizations can create systems and processes that naturally encourage secure behaviors. The promotion of security champions within teams can also further embed security awareness into the fabric of business operations.

The responsibility for maintaining a secure environment extends beyond the cybersecurity function or the Chief Information Security Officer (CISO). It is a collective responsibility that requires the engagement and participation of every employee. By instilling a culture where security is viewed as a shared obligation, organizations can create a more resilient and vigilant workforce capable of defending against cyberthreats.

TECHNOLOGY AND HUMAN OVERSIGHT

While technology plays a vital role in supporting good security habits through tools such as two-factor authentication and password managers, human oversight remains indispensable. Employees must be trained to understand the limitations of these tools and to remain vigilant in their daily activities, ensuring that security practices are consistently applied.

The balance between automating security processes and maintaining human oversight is particularly important in the context of Zero Trust models. These models, which integrate privacy, security, and cyber resilience, rely on a combination of technology and human insight to verify trustworthiness and manage access to sensitive resources.

Evaluating the effectiveness of security awareness programs is critical to ensuring that they are meeting their objectives. Organizations should employ strategies for continuous improvement, staying abreast of emerging threats and adapting their programs to address the evolving cybersecurity landscape.

SECURING THE FUTURE

Fostering a culture of security and privacy awareness is a collective endeavor that requires the active participation of every individual within an organization. By integrating the human element into IT risk management strategies, organizations can build a resilient defense against cyberthreats.

Continuous education and cultural evolution are imperative in promoting this balanced approach in risk management, ensuring that organizations remain vigilant and prepared to face the rapidly evolving cybersecurity challenges of the digital age.

This article is for general information only and is not a substitute for professional advice where the facts and circumstances warrant. The views and opinions expressed above are those of the authors and do not necessarily represent the views of SGV & Co.

JOSEPH IAN M. CANLAS is a risk consulting partner and ASEAN core consulting quality leader, and CHRISTIANE JOYMIEL C. SAY-MENDOZA is a risk consulting partner, both of SGV & Co.