



Hedayet Ullah

**SUKANTA HALDER**

In order to feed a growing population with ever diminishing farmland, the country's agriculture has undergone a notable transformation since independence, buoyed by high yielding varieties, chemical fertilisers, and pesticides.

Now, technologies such as drones and artificial intelligence in farming can play a role in increasing productivity further and promoting sustainability.

But challenges remain, ranging from erratic weather and fluctuating crop prices to limited awareness among farmers about quality seeds and pesticides, as well as the recent devaluation of the local currency, taka, according to Hedayet Ullah, managing director of Syngenta Bangladesh Limited.

In an interview with The Daily Star, Hedayet said that Bangladesh, like many of its Asian neighbours, is shifting from subsistence farming towards a more commercial model.

"It is a transformation from manual labour to mechanisation, from broadcasting pesticides to precision spraying, and from traditional farming methods to data-driven approaches using AI," said Hedayet.

To facilitate this transition, he said Syngenta Bangladesh is offering low-cost harvester services to help farmers adapt to mechanisation. "We want them to get comfortable with the technology," he said.

The leading local agri-input maker recently launched the "CropWise Grower" mobile app, allowing farmers to diagnose crop issues, monitor weather forecasts, and take timely action.

Headquartered in Switzerland, Syngenta globally supports millions of farmers in producing safe, nutritious food while caring for the environment.

In Bangladesh, Syngenta AG Switzerland holds a 60 percent stake in the joint venture, while the remaining 40 percent is owned by the government through the Bangladesh Chemical Industries Corporation (BCIC).

The company has been operating in Bangladesh for more than five decades.

According to Hedayet, Syngenta Bangladesh is committed to constant innovation to empower farmers, enhance sustainability, and contribute to food security.

As part of this strategy, the company has applied for government approval to use drones for tasks such as pesticide

spraying and fertiliser application, which will ensure more accurate and safe usage.

Meanwhile, the company plans to set up 30 "CENTRIGO Centres" in major agricultural areas by 2027, with the goal of bringing 50,000 farmers under its agri-ecosystem platform.

"This model helps farmers improve productivity, cut down risks, and increase profits through sustainable, profitable farming practices," said the Syngenta Bangladesh managing director.

These services enable farmers to harvest rice and wheat at the right time, reducing costs by 20 to 30 percent," said Hedayet. "By cutting production costs

simultaneously advancing sustainability and food security," he added.

Through CENTRIGO, farmers can access quality seeds, fertilisers, crop protection solutions, insurance, collateral-free loans, telemedicine, and mechanised services including combined harvesters.

These services enable farmers to harvest rice and wheat at the right time, reducing costs by 20 to 30 percent," said Hedayet. "By cutting production costs

future food security remains a serious concern, especially with the population continuing to rise while cultivated land shrinks, Hedayet said.

Apart from CENTRIGO, Syngenta Bangladesh is rolling out several sustainability initiatives aligned with global goals of "improving rural prosperity" and "regenerating soil and nature."

One such initiative is the "GoGrow" project, which aims to combat the

## TAKEAWAYS FROM INTERVIEW

### TECHNOLOGY & INNOVATION

Syngenta introduced mobile app to help farmers monitor crops and access weather forecasts

It has applied for govt approval to use drones for precise pesticide and fertiliser applications

It offers affordable mechanised harvesting services that reduce farmers' costs by 20-30%

### BUSINESS STRATEGY & EXPANSION

Syngenta plans to set up 30 CENTRIGO centres nationwide by 2027 to support 50,000 farmers

The company is transitioning from an input seller to a provider of "360 solutions" that include seeds, fertilisers, insurance, and healthcare services

Syngenta's partnerships with PepsiCo, MGI, and other companies help ensure fair prices for farm produce

### SUSTAINABILITY & FOOD SECURITY

GoGrow project supports over 340 coastal families in saline-prone Shyamnagar to adapt to climate change

### COMMUNITY ENGAGEMENT

Around 120,000 farmers are engaged daily by Syngenta's field force for training

SheShines initiative empowers rural women with agronomic training and financial literacy

## Rethinking cybersecurity for resilient financial systems

MAMUN RASHID

Globally, the financial sector has become a prime target for cybercrime, with attacks growing in scale, sophistication, and impact. In 2025, several high-profile breaches exposed vulnerabilities even within well-established institutions. One alarming case involved the US indictment of members behind the Qakbot malware network, which infiltrated thousands of financial systems to deploy ransomware and steal banking credentials. In Europe, a breach at a cloud platform allegedly compromised millions of encrypted financial records, prompting serious concerns about cloud infrastructure security. Similarly, Asia has witnessed targeted phishing and malware campaigns against banks and fintech firms, especially those with minimal cybersecurity investment.

In Bangladesh, fraudsters are exploiting banks and mobile financial services (MFS) by calling from numbers resembling official customer care lines. Targeting senior citizens and non-tech-savvy users, they claim accidental money transfers and request One-Time Passwords (OTP), often mimicking official messages, to gain unauthorised access and cash out funds. These incidents result in financial losses and erode public trust in the system. As cyber threats evolve, financial institutions must prioritise resilience, investing in AI-driven security, real-time threat detection, and global collaboration to safeguard integrity.

Banks are attractive targets for cybercriminals, not just because they store vast sums of money, but also because they hold sensitive customer data. Attacks are becoming more advanced, using tactics like social engineering, zero-day exploits, and exploiting systemic misconfigurations. Cyber threats are no longer static; they evolve rapidly, often outpacing even the best-prepared defences. Today's cybercriminals are well-funded, highly organised, and often operate across borders.

Historically, many financial institutions have taken a reactive stance, responding to incidents as they occur. This approach is no longer sustainable. Banks must invest in both defensive (blue team) and offensive (red team) capabilities. Regular cyberattack simulations, akin to "stress testing," are essential to prepare for real-world scenarios. Shifting to a proactive model means anticipating threats and fortifying systems before breaches occur.

Digital transformation is reshaping banking through fintech, cloud adoption, and AI integration. With the shift to online onboarding processes like Know Your Customer (KYC), securing customer data and identity is more important than ever. However, these advancements also introduce new vulnerabilities. Cybersecurity must be integrated throughout the digital journey, not as a final step, but as a continuous process.

Despite technological safeguards, the "human factor" remains a critical vulnerability. Social engineering attacks, such as phishing, exploit human error and curiosity. This underscores the need for ongoing education and awareness at every organisational level. National-level initiatives to improve cybersecurity awareness among the general public, including teachers, parents, and civil servants, are vital for creating a more secure digital ecosystem.

Amid discussions of advanced threats, the basics must not be overlooked. Many breaches still occur due to outdated software, unpatched systems, weak passwords, and poor access control. Strong cybersecurity begins with sound fundamentals such as encryption, system hardening, and full compliance with regulatory standards. While the financial sector is heavily regulated, institutions should aim to exceed minimum standards. Regulations should not be seen as a burden, but as a framework for achieving cybersecurity maturity.

Cybersecurity should not be viewed as a barrier to innovation but as an enabler. By integrating security into product development and digital services, banks can adopt new technologies confidently while maintaining customer trust.

In an era where data is currency and threats are constant, cybersecurity in banking is more than an operational requirement. It is the foundation of trust and resilience. By investing in people, processes, and technologies and fostering a culture of security, we can protect the digital future of finance.

The writer is the chairman of Financial Excellence Ltd

## Atlas to launch electric bike

**STAR BUSINESS REPORT**

Atlas Bangladesh Ltd (ABL) has partnered with Chinese electric vehicle maker Zhejiang Luyuan Electric Vehicle Company Ltd to assemble and manufacture electric scooters and bikes under the former's brand name, Atlas EV.

Under the agreement, ABL will receive technical cooperation from Zhejiang Luyuan to locally assemble and manufacture electric two-wheelers.

The company aims to begin sales through its dealer network by August this year, following the completion of necessary processes.

Atlas signed a memorandum of understanding with the Chinese company in this regard at a programme at the BSEC Bhaban in Dhaka on May 22, according to a disclosure posted on the Dhaka Stock Exchange (DSE) website.

ABL is a state-owned enterprise under the Bangladesh Steel and Engineering Corporation (BSEC) of the industries ministry.

The company began operations in 1966 in collaboration with Japan's Honda Motor Company under private ownership and was later nationalised in 1972 following Bangladesh's independence.

ABL partnered with Hero Honda in 1993, but the collaboration came to an end in 2010 when Honda and Hero dissolved their joint venture.

As of April 30, 2025, the government held a 51 percent stake in ABL, while institutional investors held 16.95 percent and the general public 32.05 percent, according to DSE data.

## Stocks extend losses

**STAR BUSINESS REPORT**

The benchmark index of the Dhaka Stock Exchange dropped 38.69 points yesterday, extending the losing run for the second consecutive day.

The DSEX lost 0.80 percent to close at 4,746.42.

The Sharia-compliant DSES index declined 0.92 percent to 1,037.23, while the DS30, which represents blue-chip stocks, dropped 1.33 percent to 1,753.29.

Turnover, a key indicator of market activity, increased 9 percent to Tk 278.02 crore compared to the previous session.

Of the issues traded, 74 advanced, 271 declined, and 52 remained unchanged.

## Gold price rises over 2%

**REUTERS**

Gold prices rose more than 2 percent on Friday and logged their best week in six, as investors sought the safe-haven asset amid renewed tariff threats from US President Donald Trump and a weaker dollar.

Spot gold gained 2.1 percent to \$3,362.70 an ounce by 1356 ET (1756 GMT). Bullion rose 5.1 percent

this week to touch an over two-week high.

US gold futures settled 2.1 percent higher at \$3,365.8.

"Trump has been on a tear the last 24 hours. Threatening 50 percent tariffs on the EU as of June 1, biting Apple and hammering Harvard has stocks in a black mood, which is great for gold," said Tai Wong, an independent metals

trader.

"Renewed tariff concerns on a low-liquidity day ahead of the long weekend can magnify moves."

Global stocks tumbled after Trump recommended 50 percent tariffs on European Union imports from June 1. Trump also said that Apple would pay a 25 percent tariff on iPhones that are sold in the US but not made there.

## How US-China chip conflict is evolving under Trump

**AFP, Beijing**

The United States has taken aim at China's Huawei over the cutting-edge chips powering artificial intelligence (AI), part of a shifting technology dispute between the two largest economies.

AFP looks at how the US-China chip war is evolving under US President Donald Trump:

A US government statement this month showed how the Trump administration is seeking to change the ways the US limits China's access to state-of-the-art semiconductors needed to develop AI.

The US Commerce Department said on May 12 that it would rescind the "AI Diffusion Rule", which was issued by Trump's predecessor Joe Biden to shield American chips from Beijing.

Set to take effect on May 15, the rule would have imposed three tiers of curbs, allowing trusted nations to freely import AI chips but controlling or banning their export to lower-tier countries like China.

It "would have stifled American innovation" while harming US diplomatic ties with "dozens of countries", the commerce department said.

The same statement reminded companies that using Huawei Ascend --

the Chinese tech giant's most advanced chip -- "violates US export controls".

It warned of "potential consequences" if US-built AI chips were used to train Chinese AI models.

The announcement aimed to "refocus the firepower" of AI curbs squarely on Beijing, said Lizzi Lee, a fellow on the Chinese economy at the Asia Society Policy Institute.

Manoj Harjani, a research fellow at Singapore's S. Rajaratnam School of International Studies, agreed, saying the policy turn meant "the spotlight (would be) clearly on China and Huawei".

Analysts told AFP that Trump's approach to chip controls marks a distinct shift from Biden. The latter relied on multilateral coordination with



Employees work at a production line manufacturing chips inside a factory in Chizhou, China.

allies to keep Beijing out of the loop, said Marina Zhang, an associate professor at the University of Technology Sydney's Australia-China Relations Institute.

In contrast, Trump's recent measures "adopt a more selective and bilateral approach", Zhang told AFP.

"(The policies are) flexible enough to accommodate allies' demands and protect US firms' global market positions, yet continue to aggressively target specific Chinese companies like Huawei through unilateral measures," she said.

Harjani noted that Trump was often viewed as a leader who "does not care much for allies and partners".

His chip policy, Harjani said, "runs counter to this assumption" as it includes efforts to create new AI-focused partnerships with allies.

Beijing has accused Washington of "bullying" and abusing export controls to "suppress and contain" China.

The fighting talk shows that Beijing "will not yield easily", Zhang said.

However, she said the restrictions would significantly hamper Huawei's access to "crucial" US chipmaking technology.

"The AI competition has entered an accelerated and potentially dangerous phase, complicating future negotiations" on global AI governance, Zhang added.