AI Strength Limits Tariff Impact on TSMC

Company's clients, such as Apple, have found supply chains increasingly strained

By Yang Jie and Joyu Wang

Taiwan Semiconductor Manufacturing Co. faces limited impact from tariffs, its chief executive said, reaffirming that artificial-intelligence demand remains strong, and the company guided for record earnings.

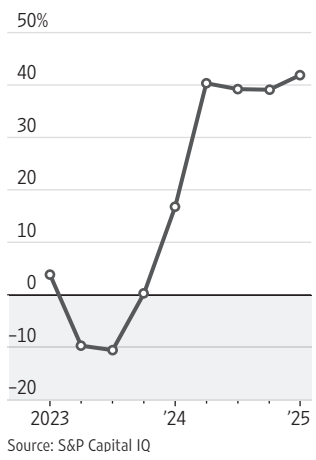
At an annual shareholders' meeting on Tuesday, Chief Executive C.C. Wei said tariffs are typically borne by importers and won't directly affect **TSMC**, the world's largest contract chip maker.

Still, he warned that if tariffs lead to a global economic downturn and higher prices, that would damp demand, indirectly affecting TSMC's business.

Top TSMC clients, including Apple and Nvidia, have found their supply chains increasingly strained amid widespread uncertainty over President Trump's trade policies. Despite this, Wei reiterated confidence in the strength of AI-driven semiconductor demand.

He expects TSMC's revenue and earnings to reach new record highs this year.

TSMC quarterly revenue, change from a year earlier



Source: S&P Capital IQ

According to Taiwan-based research firm DigiTimes, TSMC and Taiwan's broader foundry industry have seen robust sales growth so far in the April-to-June quarter. That's thanks to continued demand for AI and high-performance computing chips, a rebound in smartphone application processor shipments, and customers' push to build up inventory to get ahead of tariffs, it said in a report Tuesday.

"AI will be something you absolutely can't live without in the future," Wei told reporters after the meeting. "As long as there's demand for AI, TSMC will always be a great company with a really promising outlook."

HHWA CHENG/AFP/GETTY IMAGES

CEO C.C. Wei expects the chip maker's revenue and earnings to climb to records this year.

Wei also addressed concerns over worker safety at the company's plants and technology theft.

A dozen protesters holding a white banner stood outside the event in TSMC's home base of Hsinchu, Taiwan, protesting a string of incidents since 2019 that resulted in deaths and injuries to workers.

"Life is precious, and public safety is paramount to us," Wei said. "We recognize areas where we fell short, and I sincerely apologize on behalf of the company."

The CEO firmly dismissed shareholders' worries about technology being stolen from TSMC's overseas operations as it expands abroad. Emphasizing robust safeguards and the complexity of its technological capabilities, he said of TSMC's intellectual property: "It cannot be stolen."

Wei elaborated that TSMC's cutting-edge tech is the product of over 10,000 research and development engineers, followed by another large team of production engineers who optimize and refine it.

"If our technology could be stolen that easily, TSMC wouldn't be where it is today," he said.

The CEO said new technologies are first implemented in a so-called mother fab in Taiwan before reaching the volume production stage. This involves deploying hundreds of engineers to TSMC's headquarters for training, and another two to three hundred workers to set up production lines abroad.

"The technologies have progressed to a point where it's beyond the capacity of an individual, 10 people, or even a hundred, to steal," he said.

Wei also denied reports that TSMC is planning to build new chip-fabrication facilities in the Middle East.

"Do you think it's possible to have customers in the Middle East? I mean, do you really think that could happen? From what I can see, it's not that easy to build up a semiconductor industry there," he said.

Even in an established location like Taiwan, building chip-making facilities requires at least two-and-half years, Wei said.

Turning to the U.S. market, Wei said that a shortage of experienced labor in Arizona, where TSMC has manufacturing operations, makes it challenging to ramp up production capacity on American soil.

He said Trump had asked if TSMC can complete its announced $100 billion investment in the U.S. within five years or so. Wei said he had told the U.S. president that this would be very difficult, to which Trump replied: "Mr. Wei, do your best."

Warner Shareholders Say No

Continued from page B1

and other streaming services.

The company is also exploring a potential spinoff of its cable networks. Last December the company said it was restructuring into two operating divisions—one focused on its streaming and movie and television production studios and the other on its cable networks.

Entertainment chieftains often have higher compensation than chief executives in other industries.

Netflix Chief Executives Ted Sarandos and Greg Peters each had compensation packages valued at more than $60 million in 2024. Disney Chief Executive Bob Iger had a pay package valued at $41.1 million.

59%

Percent of Warner shareholders who cast votes against CEO's pay package.

Shareholders at other entertainment companies have also expressed disapproval of the compensation, in nonbinding votes.

In 2023, Netflix shareholders voted against the pay compensation of its top executives including Sarandos, Peters and Chairman Reed Hastings.

In 2018, Disney shareholders voted against Iger's compensation plan.

CrowdStrike Swings to Loss

By Katherine Hamilton

CrowdStrike swung to a loss in the fiscal first quarter as the costs of its outage last summer continue to weigh on results.

The cybersecurity company on Tuesday posted a loss of $110.2 million, or 44 cents a share, in the quarter ended April 30, compared with a profit of $42.8 million, or 17 cents a share, a year earlier.

Stripping out certain one-time items, adjusted per-share earnings were 73 cents, ahead of the 66 cents forecast by analysts, according to FactSet.

Revenue rose 20% to $1.10 billion. Analysts surveyed by FactSet forecast revenue of $$1.11 billion. That growth was driven by subscription revenue, which increased 20% to $1.05 billion.

CrowdStrike logged a $38.7 million expense from general and administrative costs associated with a widespread software outage last July. It also spent $537 million on research and development expenses related to the incident.

CrowdStrike has been giving out special incentives to try to hang onto customers after the software outage. Those incentives let customers try some products for free, and were still weighing on CrowdStrike's earnings in the fourth quarter.

Management has previously said the company wouldn't return to growth until the fall.

Victoria's Secret, North Face And Cartier Log Cyber Attacks

By Suzanne Kapner

A string of recent cyber attacks has targeted big retailers, scooping up customer information and disrupting online sales.

North Face and Cartier in recent days told customers that their names and email addresses had been stolen. Another cyber intrusion prompted Victoria's Secret to shut down its website for three days and postpone the quarterly earnings announcement that it had planned for this week.

The disclosures by North Face, Cartier and Victoria's Secret follow a spate of attacks against U.K. retailers that appear to have been perpetrated by a group known as Scattered Spider. Members of the hacking group pretend to be employees locked out of their corporate accounts. They then convince a corporate help desk to reset their password, a technique known as social engineering.

U.K. retailers Harrods, Marks & Spencer and Co-op all have reported cyber intrusions in recent months. Scattered Spider hasn't been publicly named as the culprit of the hacks, but is suspected in at least some of them, The Wall Street Journal has reported.

ADRIENNE GRUNWALD FOR WSJ

Victoria's Secret delayed reporting its results after the breach.

North Face, which discovered a breach on April 23, said it was the target of a different type of attack known as credential stuffing. Hackers used account authentication credentials such as addresses, usernames and passwords that were stolen from another source to gain unauthorized access to user accounts, North Face said. Credential stuffing can occur when people use the same passwords on multiple websites.

"Based on our investigation, we believe that the attacker previously gained access to your email address and password from another source (not from us) and then used those same credentials to access your account on our website," North Face told customers in an email last week.

It is unclear what techniques were used in the Cartier and Victoria's Secret breaches.

In an email to customers, Cartier said that some client names, email addresses, countries of residence and birth dates may have been stolen. No passwords, credit card details or other banking information were affected, the company said.

Victoria's Secret shut down its corporate systems and e-commerce site on May 26. Its website was restored on May 29.

The lingerie seller Tuesday said that the incident didn't affect its financial results in the latest quarter. The company said it had to postpone its earnings announcement because the restoration processes had prevented employees from accessing information they needed to prepare the results for release.

"Companies have to sometimes break certain things to stop the attacker from getting deeper into their network," said Charles Carmakal, the chief technology officer at cyber security firm Mandiant, speaking generally and not about any specific retailer.

Listen to a Podcast: Are EVs The Future of GM?

ANDREJ IVANOV/BLOOMBERG NEWS

Mary Barra says GM remains committed to an electric-vehicle future, despite lobbying to repeal California's emissions rules and backpedaling on plans for an EV motor plant. **Scan this code** for the WSJ podcast.