

## SAMSUNG LEADER LEE GIVEN 5-YEAR JAIL SENTENCE

**SEOUL:** The billionaire head of South Korea's Samsung Group, Jae Y. Lee, was sentenced to five years in jail for bribery on Friday in a watershed for the country's decades-long economic order dominated by powerful, family-run conglomerates. After a six-month trial over a scandal that brought down the then president, Park Geun-hye, a court ruled that Lee had paid bribes in anticipation of favours from Park. The court also found Lee guilty of hiding assets abroad, embezzlement and perjury.

Lee, the 49-year-old heir to one of the world's biggest corporate empires, has been held since February on charges that he bribed Park to help secure control of a conglomerate that owns Samsung Electronics, the world's leading smartphone and chip maker, and has interests ranging from drugs and home appliances to insurance and hotels. Lee, who emerged stony-faced from the Seoul courtroom in a dark suit, but without a tie, and holding a document envelope, was escorted by justice ministry officials back to his detention centre.

"This case is a matter of Lee Jae-yong and Samsung Group executives, who had been steadily preparing for Lee's succession ... bribing the president," Seoul Central District Court Judge Kim Jin-dong said, using Lee's Korean name. Kim said that as the group's heir apparent, Lee "stood to benefit the most" from any political favours for Samsung. Lee denied

wrongdoing, and one of his lawyers, Song Wu-cheol, said he would appeal. "The entire guilty verdict is unacceptable," Song said, adding he was confident his client's innocence would be affirmed by a higher court. The case is expected to be appealed all the way up to the Supreme Court, likely next year. The five-year-sentence - one of the longest given to a South Korean business leader - is a landmark for South Korea, where the family-run conglomerates - or chaebols - have long been revered for helping transform the once war-ravaged country into a global economic powerhouse. But they have more recently been criticized for holding back the economy and stifling small businesses and start-ups. Samsung, a symbol of the country's rise from poverty following the 1950-53 Korean War, has come to epitomize the cosy and sometimes corrupt ties between politicians and the chaebols.

### Precedent

"The ruling is a turning point for chaebols," said Chang Sea-jin, a business professor at Korea Advanced Institute of Science and Technology. "In the past, chaebols weren't afraid of laws because they were lenient. Now, Lee's ruling sets a precedent for strict enforcement of laws, and chaebols should be wary." Under South Korean law, sentences of more than three years cannot be suspended. LEADERSHIP VACUUM The third-generation de facto



**SEOUL:** Samsung Electronics Co Vice Chairman Lee Jae-yong (right) leaves after his verdict trial at the Seoul Central District Court on Friday in Seoul. —AP

head of the powerful Samsung Group, Lee has effectively directed operations since his father, Lee Kun-hee, was incapacitated by a heart attack in 2014.

Some investors worry a prolonged leadership vacuum could slow decision-making at the group, which has more than five dozen affiliate companies and assets of 363.2 trillion won (\$322.13 billion). Its listed companies make up about 30 percent of the market value of South Korea's KOSPI stock index. Many tycoons, including Lee's father, were convicted of crimes in the past, ranging from bribery, embezzlement and tax evasion, only to get presi-

dential pardons, as both the government and the public feared going too hard on them would hurt the economy. But South Korea's new liberal president, Moon Jae-in, who won a May election, has pledged to rein in the chaebols, empower minority shareholders and end the practice of pardoning tycoons convicted of white-collar crime. The presidential Blue House said in a statement that it hopes the ruling will serve as an opportunity to "end the nexus of business and politics that has held back the country."

### Transparency

In a June interview with

Reuters, Moon said he did not believe Samsung's operations depended just on Lee. "When Lee was taken into custody, the share prices of Samsung went up," Moon said. "If we were to succeed in reforming the running of the chaebols and also increasing transparency, I believe this will not only help the economic power of Korea but also help to make the chaebols themselves more competitive."

Investors say shares in chaebol companies trade at lower prices than they would otherwise because of their opaque corporate governance - the so-called Korea Discount. Shares of Samsung Electronics dropped more than 1 percent, and other group companies, including Samsung C&T and Samsung SDS, also turned lower after the verdict. The court said Samsung's financial support of entities backed by a friend of Park's, Choi Soon-sil, constituted bribery, including 7.2 billion won (\$6.4 million) in sponsoring the equestrian career of Choi's daughter. In return, prosecutors say, Samsung sought government support for the 2015 merger of two of its affiliates, which helped Lee tighten control of the conglomerate. His lawyers had argued that the merger was done for business reasons.

Some criminal lawyers had expected Lee to be found innocent of the major charges, as much of the evidence at the trial has been circumstantial. The appeals court and the Supreme

Court might put a greater emphasis on prosecutors to provide direct proof of quid pro quo, the lawyers said. PARK SUPPORTERS OUTRAGED Park, who was forced from office in March, faces her own corruption trial, with a ruling expected later this year. Prosecutors have argued that Park and Lee took part in the same act of bribery - so Lee's conviction would appear ominous for the former president. Hundreds of Park's diehard supporters who rallied outside the court on Friday reacted with outrage to the ruling. "Our ultimate goal is Park's acquittal and release," Kim Won-joon, a 62-year-old former construction worker said.

"We worry how today's guilty verdict for Lee would affect Park's ruling." Such supporters are a minority compared with the huge crowds that turned out in Seoul every week to call for Park's ouster after the bribery scandal surfaced late last year. Public approval of Lee's prosecution may underscore growing frustration in Asia's fourth-largest economy that the wealth amassed by conglomerates has not trickled down. "I think it was difficult for a court to ignore public opinion, given that the scandal rocked the country," said Chung Sun-suk, chief executive of research firm Chaebol.com. "The five-year sentence was low given that he was found guilty of all the charges. I think the court gave him a lighter sentence, taking into account Samsung's importance to the economy."—Reuters



**COLOGNE:** Fantasy game characters are seen during gaming fair "gamescom". —AFP photos



**COLOGNE:** This file photo shows people dressed up as game characters during the opening ceremony of gaming fair "gamescom" in Cologne, western Germany.

## ESPORTS HOPEFULS DARE TO DREAM BIG AT GAMESCOM

### GAMERS SURGE THROUGH COLOGNE'S TRADE FAIR

**COLOGNE, Germany:** As hundreds of thousands of gamers surge through the halls of Cologne's Gamescom trade fair, a select band ducks out of the throng into roped-off lounges and VIP sections to talk tactics and prize money—the professional eSports players.

Fast becoming one of the biggest trends in gaming, eSports sees teams of professional computer game players battle it out for cash prizes in front of giant audiences online or in real-life arenas with tens of thousands of seats. A slightly-built 23-year-old from Slovakia, Martin Styk could easily have passed unnoticed at an event like Gamescom if it weren't for his bright red football-style shirt emblazoned with the logos of big-name sponsors like Vodafone and Dr. Pepper.

Under his online alter-ego Styko, German eSports team mousesports hired him in early August for his skills in the tactical shooter game Counter-Strike that pits insurgents against counter-terrorists. "It's definitely not an easy task to become this kind of a player, but I can say so far it's really worth it," he said across the barrier to a VIP area punctuated elsewhere by gawkers angling for a view into the lives of the energy drink-sipping pros.

Styk spends up to 10 hours a day practicing his chosen game, a rhythm he's kept up for around two years since eSports became his full-time job. On top of keeping their skills sharp, professional players maintain intense interaction with their fans, streaming live video of their playing sessions while chatting about their performance and post-

ing a steady flow of tweets. Even with the pressure to perform and to be available to fans, perks for an eSports pro can be attractive, with all-expenses-paid travel to tournaments or events like Gamescom, where mousesports played friendly matches against rival team Flipsid3 Tactics.

"We as the players are kind of living the dream while we're on the road. It's something that maybe will not last forever, but since I have it I want to enjoy it as much as I can," Styk said.

### Billion dollar business

Dane Saief Al-Faour-whose team Meet Your Makers claimed the title of world champions in Battlefield 4 at Gamescom 2014 — was a little more cautious at the height of his gaming career. Now 32, he never quit his job as a software developer even back when prize money was rolling in.

That turned out to be the safer choice, as the combat game's star faded and the cash dried up. "I've always been a hardcore Battlefield fan. I don't play for money. If I played for money then I would play something else," Al-Faour explained. The most popular games can be lucrative. At Gamescom, some \$237,000 (200,000 euros) was set to be distributed among winners of a Rainbow Six league, while contenders in a Playerunknown's Battlegrounds league had their sights on total prize money of \$350,000.

Al-Faour still nurtures hope that the latest installment of the Battlefield franchise will propel the series back into big-time competitions. But he's

equally enthusiastic about other possibilities opening up in the field. eSports "is changing a lot and we don't know where it's gonna take us, what the limit is," he said. Estimates cited by the organisers of the E3 industry show in July suggest eSports could hit the threshold of \$1 billion in revenue next year, five times its size in 2015. eSports will be an official part of the Asian Games in Hangzhou, China in 2022 after a dry run at next year's event-although the oft-discussed prospect of gaming securing a place at the Olympics still appears remote.

### Passion project

And with more cash and larger crowds come new opportunities for insiders, like working as a talent spotter for big-name teams or offering on-camera analysis of live events. "I'm getting too old for the game personally, but I would like to be more involved. I need to go for my passion, and my passion is eSports," Al-Faour said. Even for those striving to break into the exclusive world of the professionals, gaming remains a passion rather than a piggy bank.

"Having a lot of money or getting a lot of fans isn't the goal. It's about playing and making people happy," said Fabian Robbe, a 21-year-old Call of Duty player from western Germany using his ample downtime as a student to hone his bid for the big leagues. In any case, "only maybe one percent of people manage" to make a living from eSports, he pointed out. "That's why I'm focusing on my studies right now." — AFP

## DIGITAL SAFEGUARDS NEEDED TO MEET INDUSTRIAL CYBER SECURITY DEMANDS IN KUWAIT

By Safdar Akhtar

**KUWAIT:** Nationwide digital transformation is expected to play a central role for Kuwait in realizing its new 2035 vision, which was announced earlier this year. The country aims to attract more than KD400 million in investments to information technology, services, and renewable energy in the short and medium term. It is widely believed that - in line with the rest of the major Gulf Corporation Council (GCC) markets - Industrial Internet of Things (IIoT), cloud technology and Big Data will drive this movement.

The region's digital markets are expanding at an overall compound annual growth rate of 12 percent and it is estimated that digitization could add as much as \$820 billion to regional GDP by 2020.

The Kuwait National Development Plan's short-to-medium term objectives include positioning Kuwait as a global hub for the petrochemical industry. The rise in digitization across Kuwait's petrochemical sector brings both opportunities for growth and challenges - particularly in a country where oil and gas remains the leading industry. With the increasing focus on cyber security threats across industrial sites, it is evident that Kuwait will need to ensure full protection of its assets and information through a greater focus on digital safeguards. It was announced in April of this year that Kuwait has enacted several legislations aimed at minimizing irregular use of emerging communication means. This comes on the back of increased cyber security threats amidst a rapid rise in technological advancement across the country. Kuwait is not alone in this regard, as organizations across the Middle East strive to create a secure digital environment.

The Middle East cyber security market size is expected to grow from \$11.38 billion in 2017 to \$22.14 billion by 2022. This is due to the increasing number of cyber incidents in the region, resulting in more focus on implementing advanced technology to combat the threats.

According to Repository of Industrial Security Incidents (RISI) data, cyberattacks against oil and gas organizations in the Middle East make up more than half of the recorded instances. Major energy players in Kuwait and across the GCC have also witnessed a rise in the number of cyberattacks in recent years. As such, businesses and government agencies in Kuwait are increasingly implementing services that help protect on-site data and information stored at remote locations.

One key area for protecting information includes USB devices on industrial sites.

Malware spread through USB devices - used by employees and contractors to patch, update and exchange data with onsite control and computer systems - is a fundamental risk for industrial control systems. It was the second leading

threat to these systems in 2016, according to BSI publications, after cyber-attacks. Uncontrolled USBs have taken power plants offline and downed turbine control workstations, among other industrial applications.

Industrial operators often have hundreds or thousands of employees and dozens of contractors on site every day. Many of those rely on USB-removable media to get their work done. Plants need solutions that allow people to work proficiently, but also don't compromise cyber security and industrial safety. Presently, many plants either ban USBs - which is difficult to enforce and significantly reduces productivity - or rely on traditional IT malware scanning solutions, which are problematic to maintain in an industrial control facility and provide inadequate protection. These systems fail to protect process control networks against the latest threats, and offer no means to address targeted or zero-day ICS attacks. New industrial cyber security innovations are now enabling secure use of USB devices, offering solutions to CIOs of oil and gas organizations across Kuwait and the region. The new innovations provide hassle-free, multi-layered protection for managing USB security, letting users simply plug in and check devices for approved use in the facility. Contractors "check-in" their USB drive by plugging it into an Intelligence Gateway. The ruggedized industrial device analyzes files using a variety of techniques included with Advanced Threat Intelligence Exchange (ATIX), a secure, hybrid-cloud threat analysis service.

For most plants, the proliferation of removable media and USB devices is unavoidable, but the security risks they bring don't have to be. The new technology provides easy and secure solution to USB security in industrial plants. It helps prevent the spread of malware through removable media; stops unverified files being read by Windows hosts; and, through the private ATIX connection, provides continually updated threat information and advanced analytics to help detect advanced, targeted, and zero-day malware. It is these types of solutions that will allow Kuwait and regional oil and gas players to ensure that they have the proper protection needed to ensure maximum cyber security. Studies show that the adoption of digital safeguards is increasing as IT spending within the Middle East oil and gas sector grew to around \$1.66 billion in 2016.

Clearly, security remains the most important area of focus for energy-sector CIOs in the region. The level of digitization in the industry is increasing, while the threat landscape is becoming increasingly multifaceted, resulting in CIOs turning more of their attention towards IT security.

For organizations within Kuwait that are keen to ensure maximum cyber security, implementing state-of-the-art solutions that protect data and information will go a long way in achieving that goal. *Note: Safdar Akhtar is Business Development Director, Industrial Cyber Security for EMEA and Asia at Honeywell Process Solutions (HPS)*

## FACEBOOK LAMBASTED OVER RANSOM VIDEO OF TRAFFICKERS ABUSING MIGRANTS

**LONDON:** People smugglers are using Facebook to broadcast the abuse and torture of migrants in order to extort ransom money from their families, the UN migration agency said on Friday.

The International Organization for Migration (IOM) lambasted the tech giant for failing to police the platform and help crack down on traffickers. One video hosted on the site since June shows Libyan gang-masters threatening emaciated and abused migrants - mostly Somalis and Ethiopians - huddled in a concrete room. IOM said the traffickers had sent clips to the captives' families via the encrypted messaging service WhatsApp - a Facebook channel - along with threats that

their loved ones would be killed unless ransoms of up to \$10,000 were paid. One young Somali man is seen lying face down with a concrete block on his back. "I was asked for \$8,000," he says, according to the IOM. "They broke my teeth. They broke my hand. I have been here 11 months. They put this stone on me for the last three days. It's really painful."

British newspaper The Times, which ran the story on its front page on Friday, also quoted a young Ethiopian who had been held for 15 months. "They beat me with iron bars," he said.

"They ordered me to pay \$8,300 and my family cannot afford to pay that amount." Hundreds of thou-

sands of refugees and migrants have crossed the Mediterranean from North Africa to Europe since 2014, and thousands have died trying.

Facebook, which has also been criticised for failing to stop traffickers using the platform to advertise their services, said posts by smuggling groups would be removed if reported. "We encourage people to keep using our reporting tools to flag this kind of behavior so it can be reviewed and swiftly removed by our global team of experts, who work with law enforcement agencies around the world," a spokesperson said. But Facebook said it had not removed the June video as it had been posted by a Somali journalist and was important for raising

awareness of the problem. However, IOM spokesman Leonard Doyle accused Facebook of "arrant nonsense", adding that the smugglers had used the journalist to publicize their demands.

He told the Thomson Reuters Foundation it was totally inappropriate for Facebook to host a video showing the faces of vulnerable people being abused. "Don't let Facebook off the hook here," he said. "It's an absolutely nonsensical argument that it's up to the public to notify Facebook of stuff that's happening on Facebook."

"They should invest heavily in policing their platforms to stop vulnerable migrants being exploited, extorted and murdered."—Reuters