On Sunday, May 30, JBS USA announced that it was the target of a major cyberattack and has shut its North American and Australian computer networks. According to a media statement, “the company took immediate action, suspending all affected systems, notifying authorities and activating the company's global network of IT professionals and third-party experts to resolve the situation. The company’s backup servers were not affected, and it is actively working with an Incident Response firm to restore its systems as soon as possible.”
JBS media contact Nikki Richardson explained that a solution will take time and that transactions with customers and suppliers could be delayed.

JBS Foods is the world’s largest beef and poultry producer and the second-largest global pork producer. The company has locations in the United States, Australia, Canada, United Kingdom, Mexico, Europe, and New Zealand. According to their website, JBS has five pork production facilities in the United States with a combined processing capacity of 92,000 hogs per day. JBS also has nine beef production facilities in the U.S. with a combined processing capacity of around 28,000 cattle per day.
JBS’s slaughter operations in Australia and Canada have already been impacted. Beef and lamb slaughter in Queensland, Victoria, New South Wales, and Tasmania had been canceled Monday. JBS Australia CEO Brent Eastwood confirmed the cyberattack and was not yet able to provide a definitive timeline on how long operations in Australia will be shuttered. In Canada, operations were affected at the company's beef plant in Brook, Alberta.

JBS is currently working with the Australian government and international partners to investigate where and who has perpetrated the attack. Australia's Agriculture Minister David Littleproud stated “the technology that [JBS] use, the systems they use, go to the heart of the quality assurance of the beef that they process. So we need to make sure that we can get that up and going to give confidence, not just to consumers here in Australia, but also to our export markets.”

As of now, it is not yet certain if slaughter operations will be impacted in the United States. The majority of beef and pork plants in the U.S. were closed Monday in observance of the Memorial Day holiday. Today is the first day that the CME is implementing $5 daily limits for live cattle futures.

The supply chain could see significant disruptions if processing facilities under JBS's umbrella are temporarily idled in the United States. If plant closures do occur and are long-lasting, cattle and hogs scheduled for slaughter would likely be rerouted to the feedlots or barns until further notice.

This cyberattack on the massive meat supplier closely follows the ransomware attack on Colonial Pipeline just three weeks ago, leading to a push to regulate cybersecurity. Meanwhile, meat processing facilities across the nation are still contending with labor shortages and worker absenteeism following the string of plant closures and slowdowns in 2020 due to the pandemic.

Urner Barry will continue to monitor the situation and will provide updates when possible.

June 2, 2021

JBS USA said the "vast majority" of its processing plants would be up and running today after the company made significant progress in resolving the Memorial Day weekend cyberattack on its operations in North America and Australia.

The White House on Tuesday said JBS notified the administration Sunday that it was the victim of a ransomware attack, and that the ransom demand came from a criminal organization likely based in Russia. The FBI is investigating the incident, U.S. Deputy Press Secretary Karine Jean-Pierre said in a press briefing.

"The White House is engaging directly with the Russian government on this matter and delivering the message that responsible states do not harbor ransomware criminals," Jean-Pierre said.
JBS said it was not aware of any evidence that any customer, supplier or employee data had been compromised.

“Our systems are coming back online and we are not sparing any resources to fight this threat. We have cybersecurity plans in place to address these types of issues and we are successfully executing those plans. Given the progress our IT professionals and plant teams have made in the last 24 hours, the vast majority of our beef, pork, poultry and prepared foods plants will be operational tomorrow,” Andre Nogueira, JBS USA chief executive, said in a statement late Tuesday.
JBS USA and its Pilgrim's unit were able to ship product from nearly all of their facilities on Tuesday to supply customers, and the JBS beef plant in Canada resumed production, the company said. Operations in Mexico and the UK were not affected and are conducting business as normal.

The company did not identify which of its facilities were affected by the cyberattack. News reports suggested as many as nine beef plants experienced shutdowns. ABC News reported that plants in Arizona, Colorado, Michigan, Nebraska, Pennsylvania, Texas, Utah and Wisconsin were shut down. In Canada, livestock slaughter was stopped at the JBS beef processing plant near Brooks, Alberta, according to CBC News. In Australia, the attack shut down operations across several Australian states, CNBC reported.

JBS USA has received strong support from the U.S., Australian and Canadian governments, conducting daily calls with officials in an effort to safeguard the food supply, the company said.

The U.S. Cybersecurity and Infrastructure Security Agency is providing technical support to help the company recover from the attack, according to the White House.
“I want to personally thank the White House, the U.S. Federal Bureau of Investigation, the U.S. Department of Agriculture, and the Australian and Canadian governments for their assistance over the last two days,” Nogueira said.
USDA has contacted several major U.S. meat processors to make sure they are aware of the situation and is assessing any impact on the food supply, the White House said.

June 3, 2021
JBS USA said it was on schedule to resume meat and poultry processing at all of its facilities today, with global operations close to full capacity, as it continues to recover from a weekend cyberattack that interrupted production across its plants in North America and Australia.

The world's largest meatpacker said the progress in restoring normal operations offers "further assurance" to its team members, livestock and poultry producer partners, customers and consumers, reiterating that it is not aware of any evidence that its data was compromised.
“JBS USA and Pilgrim's continue to make significant progress in restoring our IT systems and returning to business as usual,” JBS USA Chief Executive Andre Nogueira said in a statement late Wednesday. “Today, the vast majority of our facilities resumed operations as we forecast yesterday, including all of our pork, poultry and prepared foods facilities around the world and the majority of our beef facilities in the U.S. and Australia.”

The ransomware attack prompted worries about tightening meat supplies if production could not be quickly restored. The Wall Street Journal reported Wednesday that the Publix Super Markets chain cautioned the plant closures could lead to chicken shortages over the next few days.

The United States Cattlemen's Association on Wednesday sent a letter to Secretary of Transportation Pete Buttigieg requesting emergency flexibility for transporters of livestock and fresh meat products to make sure grocery stores remain stocked in the wake of the cyberattack.
Media reports said all nine JBS beef plants in the U.S. experienced shutdowns, while production was scaled back at five of its six pork facilities and some Pilgrim's Pride chicken plants.
President Joe Biden told reporters Wednesday that his administration was "looking closely" at whether the U.S. would retaliate for the cyberattack, NBC News reported. The White House on Tuesday said the ransom demand came from a criminal group likely based in Russia.

White House press secretary Jen Psaki said Biden will raise the issue of cyberattacks by Russia-based hackers when he meets with Russian President Vladimir Putin in two weeks.
Australia's agriculture minister told CNN Business Wednesday that he did not anticipate a red meat shortage, even though JBS accounts for about a quarter of processing in the country.

June 4, 2021

JBS USA on Thursday said all of its global facilities are fully operational after the resolution of a cyberattack on its computer servers that disrupted the company's meat and poultry processing operations in North America and Australia.

Lost production from the attack was limited to less than one day's worth across the global business, and that output will be fully recovered by the end of next week, the company said in an announcement.

The FBI in a statement Wednesday attributed the ransomware attack on JBS to REvil, a criminal organization likely based in Russia. Forbes reported that the group licenses its malware to affiliates and has taken credit for several cyberattacks, including claiming last month to have hacked into the system of a supplier to Apple.

JBS provided new details on its response to the attack, saying it immediately contacted federal officials and activated its cybersecurity protocols, including voluntarily shutting down all of its systems, to isolate the intrusion. Those steps limited potential infection and preserved core systems, the company said.

Its encrypted backup servers were not infected during the attack, which allowed for a return to operations sooner than expected, the company said. JBS and its Pilgrim's unit prioritized restoring systems critical to production to ensure the food supply chain.

"The criminals were never able to access our core systems, which greatly reduced potential impact. Today, we are fortunate that all of our facilities around the globe are operating at normal capacity, and we are focused on fulfilling our responsibility to produce safe, high-quality food," JBS USA Chief Executive Andre Nogueira said.

The FBI said it is working to bring those responsible for the JBS attack to justice. The White House this week said President Joe Biden would raise the issue of the growing threat from cyberattacks with Russian President Vladimir Putin when the two meet later this month.