Cybersecurity

Key Takeaways

- Recent cyberattacks on JBS Foods and Colonial Pipeline raised awareness to vulnerabilities in the supply chain and national security.
- USDA's estimated daily livestock slaughter report showed drops in processing of about 27,000 cattle and about 95,000 hogs from the week prior to the hack on JBS Foods.
- The agriculture sector faced a great threat as the attack on Colonial Pipeline occurred in the midst of planting season.

Questions

1. How were farms in your community impacted by the cyberattacks on JBS Foods and Colonial Pipeline?
2. Does your farm have a security plan?
3. What resources do you need to develop a cybersecurity plan?
4. What are your vulnerabilities to cyberattacks?
5. What policy does Farm Bureau need regarding cybersecurity?

USDA's estimated daily livestock slaughter report showed drops in processing of about 27,000 cattle and about 95,000 hogs from the week prior to the hack.

Background

Recent cyberattacks on JBS Foods and Colonial Pipeline raised awareness to vulnerabilities in the supply chain and national security. These attacks led to market disruptions and panic among consumers. Farmers were put in a bind as the southern region experienced a week-long fuel shortage in the midst of planting season and even more pronounced backlogs in the meat processing sector. With the advancement of data-driven precision ag tools, agriculture's vulnerability to cyberattacks is on the rise.

JBS is one of the so-called "big four" beef packers and represents just about a quarter of the nation's beef processing capacity. The company's processing system is largely reliant on its computer systems for recordkeeping, regulatory reports, sorting livestock, and many other aspects of meat processing. According to the Brazilian-based company, JBS has "65 production facilities, 44 prepared foods facilities, six feedlots, six live hog operations and eight transportation terminals with operations in 28 U.S. states, Canada, Puerto Rico, Mexico, Europe, Australia and New Zealand." Those facilities employ more than 100,000 people and have the ability to process more than 200,000 cattle, 500,000 hogs, 45 million chickens, and 80,000 combined lambs, sheep, goats, and veal calves per week.

According to media reports, the shutdown of JBS Foods forced about 7,000 workers in its Australian processing facilities to halt work. JBS also canceled shifts and turned away livestock haulers at its large U.S. and Canadian meatpacking plants while the company's U.S. processing operations were taken offline. **USDA's estimated daily livestock slaughter report showed drops in processing of about 27,000 cattle and about 95,000 hogs from the week prior to the hack.**

Colonial Pipeline is the United States' largest fuel pipeline. In May, the operator of the pipeline fell prey to a ransomware attack, forcing operations to stop. While the pipeline was at or near full capacity, fuel could not be released for risk of a further data breach which would potentially jeopardize the entire company's operations, including its employees' personal information. All consumers in the southeast were impacted by this attack. Many gas stations quickly ran out of fuel due to panic buying from consumers. **Most importantly, the agriculture sector faced a great threat as this occurred in the midst of planting season.** While operations resumed within a week, this event revealed fragility within the nation's infrastructure system in regard to cybersecurity.

Conclusion

Whether it is infrastructure, off-road equipment and machinery, high-tech food and grain processing, radio frequency ID-tagged livestock, or global-positioning-system tracking, the agriculture sector depends on information systems to sustain and improve operations, competitiveness, and profitability. **Embracing technology comes with risks, and the sector finds itself targeted as never before, because of its intellectual property being coveted by foreign competitors.** Until recently, most food and agriculture companies did not invest in cybersecurity defense and were lax in fortifying their infrastructure and developing sound cybersecurity practices. Recent cyberattacks have only exacerbated the vulnerability in the agriculture sector.

Steps to Take on the Farm

According to a report from the Federal Bureau of Investigation (FBI), these steps can help shore up potential vulnerabilities in your data security at the farm level:

- **Be proactive and actively manage data.** Be proactive with and accountable for the steps you can take to keep your data secure. Perform recommended software updates, frequently change account passwords, and regularly check application and platform security settings to help ensure you are equipping yourself with the latest security tools.
- **Choose the right platforms.** Research your options for managing your farm data. Consider paying even a small monthly fee for stronger security settings. The right decision is a balance between expense and your data security expectations.
- **Store your data right.** Where and how you store your data is important to its security from potential cyberattacks. If stored in the cloud, make sure the platform has adequate security protocols. If doing so locally, use a storage device with firewalls in places not connected to the internet.
- **Involve your whole team.** Create processes to manage the increasing volume of data gleaned by today's precision ag tools. Staying up-to-date with the latest and most effective data security tools and platforms is not easy for everyone. Meet with employees and other farm stakeholders regularly to ensure everyone is on the same page to keep your data secure.

Most importantly, the agriculture sector faced a great threat as this occurred in the midst of planting season.

Embracing technology comes with risks, and the sector finds itself targeted as never before, because of its intellectual property being coveted by foreign competitors.