Cybersecurity and AgTech

July 13, 2021 Roger Royse, Gavin George

PRACTICES Agriculture Technology, Privacy and Cybersecurity

The recent ransomware attack on the Colonial Pipeline, the largest gasoline pipeline in the United States, has accentuated the vulnerabilities of technology-based critical infrastructure. It has long been known that the supply chain is vulnerable to cyberattacks. In 2017, for example, the shipping giant Maersk was a victim of the NotPetya ransomware. The COVID-19 pandemic has placed even more stress on the supply chain and, as agriculture has become tech-enabled, farmers and agriculture technology providers (ATPs) have become more exposed to cyberattacks. There was a time when the biggest cyber risk to AgTech was data breach and loss of trade secrets, but as farms become wired, especially with the expansion of rural broadband access, farmers must consider the operational risks of interference with networks and devices.

The first line of defense, of course, is to have good cyber hygiene. In fact, there are already a handful of laws that require an AgTech organization to maintain reasonable cybersecurity procedures. California's Internet of Things (IoT) cybersecurity law, for example, requires manufacturers of IoT devices to provide reasonable security features to protect user privacy.[1] That law defines a reasonable security feature as a feature that is appropriate to the nature and function of the device, appropriate to the information the device may collect, contain or transmit and designed to protect the device and any information contained on the device from unauthorized access, destruction, use, modification or disclosure.

California has also long had laws requiring disclosure of data breaches involving personal information under the California Consumer Privacy Act (CCPA). Similarly, New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) protects New York residents against data breaches affecting their private information.

With the rise of the AgTech, it is only matter of time before we see malicious cyberattacks on the nation's food supply. Farmers and ATPs alike should be prepared to deal with ransomware, security and data breaches and cyber attacks.

Read more about the Privacy and Data Security Practice at Haynes Boone.

[1] California Internet of Things Cybersecurity Improvement Act of 2017. Civil Code § 1798.91.04.