The agricultural sector is increasingly a target of cyber attacks

Decades ago, when the two of us were growing up, farmers used gravity-flow gas barrels to refuel gasoline engines, rather than the fancy under-ground tanks commonly used today. Every so often, mischievous teenagers figured out that if they waited until everyone was in town, sneaked in, and filled up their cars no one would know the difference.

Once a targeted farmer grasped what was happening, a padlock was put on the nozzle. Problem solved. The same was true with missing tools. Farmers had to begin to put locks on their shop doors.

In those days, someone had to come onto the farm to steal something of value. Today that is no longer true because the most valuable thing most people have on the farm is the information contained on their computer. The threat can come in on the same wires that farmers use to connect to the internet. As these electronic systems control more things (HVAC systems, doorbells, monitoring cameras, and the list goes on), the potential vulnerabilities increase.

Malicious actors can enter using the same wire or wireless protocol that make these systems possible and never step foot on a farmer's property. They can be sitting in the basement of a nearby town or in a country half-way around the world.

In cases like the presence of "old-fashioned" malware on a home/farm computer system, the cost of an attack is generally limited to the potential loss of information as well as the time and expense it takes to get the system back up and running. These hackers were not creating chaos to make money but simply to prove that they could do it.

But the hackers of a couple decades ago have evolved into sophisticated enterprises that are out to make money off their ability to gain control of computer systems.

It was with these professional hackers in mind that the FBI (US Federal Bureau of Investigation) issued a Private Industry Notification on September 1, 2021 titled, "Cyber Criminal Actors Targeting the Food and Agriculture Sector with Ransomware Attacks" (https://tinyurl.com/jv6a6bye).

The FBI writes, "The Food and Agriculture sector is among the critical infrastructure sectors increasingly targeted by cyberattacks. As the sector moves to adopt more smart technologies and internet of things (IoT) processes the attack surface increases. Larger businesses are targeted based on their perceived ability to pay higher ransom demands, while smaller entities may be seen as soft targets, particularly those in the earlier stages of digitizing their processes, according to a private industry report."

Most of the work in hardening industrial computer systems against these ransomware attacks needs to be done by the companies in the food and processing industries. Farmers, on the other hand, should develop contingency plans in case they have to hold their grain or animals for a week or two while the purchasing company gets their systems back up and running.

The issue at that point becomes not only one of where to hold the product they cannot sell, but also the financial issue of the absence of an expected payment. Many farms run on a relatively tight budget and a couple of weeks delay in income along with continued feeding and storage costs can create a real headache.

But the problem does not stop there. What if the threat actor gets into the computer system of an equipment manufacturer and fiddles with the software used to operate a given piece of farm equipment making it inoperable? Is this possible? We don't have an answer, but we

believe there is someone out there right now who is attempting to do that. And if they are successful, the farmer's machine might become inoperable or at the very least the threat actor has access to every bit of information that piece of equipment has uploaded to the manufacturer. It is hard to imagine what they could do with that information, but they will certainly try and turn it into money for themselves.

The FBI notification provides a long list of "steps [that] can be implemented to mitigate the threat and protect against ransomware attacks," but it does not discuss how clients of the companies under attack protect themselves against the secondary ramifications of locked systems and data breaches.

As we think about it, we believe that despite their political differences the general farm organizations and commodity groups need to come together and develop a strategy to deal with the secondary impacts (farm level) of ransomware attacks on agricultural processors, suppliers, and equipment manufacturers. To do less is to leave farmers like sitting ducks on a crisp fall morning.

Policy Pennings Column 1094

Originally published in MidAmerica Farmer Grower, Vol. 37, No. 340, September 17, 2021

Dr. Harwood D. Schaffer: Adjunct Research Assistant Professor, Sociology Department, University of Tennessee and Director, Agricultural Policy Analysis Center. Dr. Daryll E. Ray: Emeritus Professor, Institute of Agriculture, University of Tennessee and Retired Director, Agricultural Policy Analysis Center.
Email: hdschaffer@utk.edu and dray@utk.edu; http://www.agpolicy.org.