Brent Johnson

Partner
801.799.5807
Salt Lake City
bjohnson@hollandhart.com

Post-Ransomware Attack: Is it Time to Return to True Systems Segmentation?

Insight — August 8, 2021

Food Logistics

This article originally appeared online by Food Logistics on August 8, 2021. Republished with permission.

In the end, food companies must balance the process efficiencies and controls that data transmission and functionality over the internet provide with the risk of cyberattacks that cripple production.

A sizeable chunk of meat production in the United States ground to a halt on June 1 when a band of hackers (or maybe just somebody in pajamas) located in Russia (or maybe Eastern Europe) launched a cyberattack against JBS USA's servers in North America and Australia. The company announced that no customer data was compromised, but customer data wasn't the point of the hack. The JBS cyber intrusion was a ransomware attack. The hackers wormed their way into the company's administrative and process control systems, encrypted them and demanded a king's ransom to give them back. Within days, JBS transferred $11 million in cryptocurrency to the virtual kidnappers to re-gain control of its systems.

Most companies have IT departments. It has become a yearly ritual to receive training on how to pepper spray cyberhackers who seemingly lurk around every corner. It is a wonder that CIOs can sleep at night knowing they are one employee click away from catastrophe.

While there are anti-phishing and malware defense tools available, there are no guarantees they work in all cases. Hackers don't have day jobs. They have nothing to do but invent new attack methods.

Companies rely on a variety of defenses to protect against ransomware attacks. These practices were recently distilled by the Biden Administration in its June 2 letter to businesses. The White House's recommendations include: (1) multi-factor authentication; (2) data encryption; (3) endpoint detection and response tools; (4) offline backup of data and systems; and (5) updating and patching systems.

It should be observed that the White House strategies focus on systems that can be hacked because they are online. At the end of the administration's letter, however, Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology, suggests process system segmentation. “It's critically important that your corporate business functions and manufacturing/production operations are separated and that

you carefully filter and limit internet access to operational networks...," she adds.

It wasn't long ago that the industry standard for manufacturing was segmentation. Process control networks were closed systems largely inaccessible from the internet. Think voting machines. Americans have been assured that hackers cannot alter elections because ballots are not recorded online (although certain voting machine manufacturers have acknowledged they place modems in some of their scanners to more quickly retrieve and relay data).

Over time, however, companies decided the business risk of not being able to access their process control networks to make adjustments to production and obtain analytics was greater than the security risk of moving their systems online. While giving manufacturers more precise control over their processes, this paradigm shift has made them vulnerable to cyberattacks.

Unfortunately, the food industry is particularly susceptible to ransomware. Unlike automotive manufacturers, which deal with relatively predictable components like steel, aluminum, fiberglass and electronics, the food industry's stock in trade are plants and animals. Organic matter is not homogenous. Product consistency demands constant monitoring. And, if the process controls are even slightly off, food and beverages end up with uninvited guests such as salmonella, e-coli, listeria, etc.

Food production also involves a wide range of discrete tasks such as cooking, boiling, centrifuging, mixing, filtering, extracting, fermenting, distilling, crushing, drying, sterilizing and pasteurizing, to name a few. All of these processes must be continuously monitored and real-time adjustments made to ensure safe and consistent products. The processes are specially designed to meet the requirements of the particular food. Sensors are placed throughout the production line to collect data, which is analyzed and reported by custom software applications. This data is not just of interest to food companies; its collection and maintenance are critical to federal regulators, such as FDA in evaluating compliance with cGMPs during 483 inspections.

The question is how much control the production team is willing to cede to allow the IT group to sleep better at night. Here are some of the options:

1. **Air gapping the production network**. Air gapping is physically isolating a network from any form of internet or LAN access. No one from the outside can hack into the network unless they are able to install malware using a portable media (a thumb drive, for example). Such malware is known as “sneakerware,” which is downloaded on foot. Air gapping creates its own challenges, such as system updates that must be done manually.
2. **Segmentation using a data diode**. Data diodes are one of the original network controls. They are “one way” hardware devices that allow data to be sent from the process control networks to the administrative networks only. The process control networks cannot be accessed from the administrative networks. Data diodes are not

completely secure, however, because there is always a possibility that hackers will find and exploit vulnerabilities in the devices. That said, data diodes create significant barriers to hacking. In established systems, the major functional problem is that the process control networks expect responses that are no longer being provided, which can cause the process control networks to malfunction.

3. **Segmentation using a next-generation firewall**. This strategy allows the policies between the process control networks and the administrative networks to be enforced and the traffic monitored. Care must be taken to limit the ports and protocols allowed to and from the process control network. Having a firewall provides little benefit if the same ports and protocols allowed on the administrative network are allowed on the process control network. Another approach to limit exposure on the process control network is to allow traffic only to specific devices. For example, if there are 200 devices on the process control network and only two need to communicate with the admin network, the firewall can limit communications to those two devices using their Internet Protocol (IP) addresses. Of course, if firewalls were the answer to hacking, almost no one would be hacked. Most companies install firewalls, but immediately start poking holes in them during the configuration process.
4. **Network segmentation using virtual local area networks (VLANs)**. This is segmenting a physical network virtually. Some food companies attempt to use VLANs as security mechanisms, and they provide some benefits. However, the benefits are limited due to the vulnerabilities with the technology and the ease that users can transverse from one VLAN segment to another. VLANs are best used to add structure to network management.

In the end, food companies must balance the process efficiencies and controls that data transmission and functionality over the internet provide with the risk of cyberattacks that cripple production. This is not an easy task by any stretch. But, food makers must be clear eyed. Their production processes are extremely sensitive, and more importantly, are participants in an industry of critical importance, making them prime targets of hackers.

Brent Johnson is a partner in Holland & Hart's Salt Lake City office. He guides clients through the complex litigation process, representing corporations in litigation matters in both the federal and state courts of California and Utah, including representing corporate defendants in class actions.
