Cyber Security Risks to the Food and Agriculture Sector

Matt Danda

Webster University

Abstract

This paper explores the cyber security risks to the Food and Agriculture (FA) sector. It begins with an overview of the FA sector and how it fits into the nation's critical infrastructure, followed by a discussion of its dependencies and interdependencies with other infrastructure sectors. The paper introduces the some of the cyber security frameworks currently in place, and then it describes methods for assessing risk. The paper then dives into a discussion of the vulnerabilities in the FA sector and, specifically, smart farming. It divides the cyber risks into four categories, and discusses the unique characteristics of each.

Introduction

The history of agriculture dates back thousands of years, and it has always played a central role in sustaining and advancing human civilization. Although only a small fraction of the modern population is engaged in farming, all of human civilization depends upon its products. Today, the world population continues to grow and demands more and more from the industry. To meet this need, farmers are turning to technology to improve efficiency and maximize yields. Although advanced technology provides many benefits, it also comes with risks and vulnerabilities. In this paper, I'll discuss the cyber risks faced by the Food and Agriculture (FA) Sector.

Definition of Food and Agriculture (FA) Sector

The FA Sector is one of the 16 critical infrastructure sectors identified by the Department of Homeland Security (DHS). These sectors are vital to the safety and security of the United States. If any of these sectors is harmed or damaged, the ability for the country to function is at risk, thereby putting social stability at risk. In simple terms, the FA Sector is responsible for farming crops and breeding animals. Its output provides food and other natural products that sustain and enhance life. The two U.S. government agencies most closely associated with the FA Sector are the U.S. Department of Agriculture (USDA) and the Department of Health and Human Services.

The FA Sector feeds the people and animals in the United States and has the capacity to export food to other countries. (DHS, 2015, p2-3) Most of this sector is privately owned, and it accounts for approximately one-fifth of the country's economic activity. According to the DHS (2015, p3), the United States had over 935,000 restaurants and approximately 114,000 grocery stores in 2014. The largest sources of revenue in the FA sector are cattle, poultry, corn, soybeans, and milk.

The FA Sector does not operate in isolation—it is dependent upon a variety of other infrastructure sectors. In addition, the FA Sector actively participates in the global economy by importing and exporting both ingredients and finished products. It plays an important role in global humanitarian efforts and maintaining worldwide food security.

Dependencies and Interdependencies

The FA Sector maintains a complex set of dependencies and interdependencies with other critical infrastructure sectors. The FA Sector is highly dependent upon other sectors, such as:

- Water. A functioning Water Sector is vital for food production, and any failures in the water supply would be devastating. (It is interesting to note, however, that the Water Sector is not dependent on the FA Sector for its functions.)
- Transportation. The Transportation Sector connects everyone in the vast supply chain required to maintain the FA Sector, which includes delivering the necessary inputs and transporting the final outputs.
- Chemical. The FA Sector relies on the Chemical Sector for fertilizers and pesticides that help optimize crop production.
- Commercial. The FA Sector relies on the Commercial Facilities Sector to sell its products.
- Financial. The Financial Services Sector provides the financial backbone of the food and agriculture industry itself. (DHS, 2015, p21-22)

The FA Sector has many interdependent relationships with other sectors. The National Infrastructure Advisory Council (NIAC) identifies interdependencies between the FA Sector and the Energy, Information Technology (IT), and Communications sectors. (DHS, 2015, p21)

All infrastructure sectors are related in some way. Lopez (p2, p40) discussed the intertwined nature of the energy and information and communication sectors. A failure in either of these sectors adversely affects pretty much every other critical infrastructure sector, including FA. The information and communication sector, in turn, relies heavily on power, transportation, and, of course, human beings (with all of their associated needs) to operate its own infrastructure. Speaking of human beings, the workers in the FA Sector are dependent upon physical security, financial services, and healthcare—as well as practically everything produced by the FA sector. (DHS, 2015, p21)

While this paper focuses on the FA Sector, it is so heavily dependent on other infrastructures, and these other sectors are so intertwined, that it is virtually impossible to consider the FA sector in isolation.

Current Security Directives and Frameworks

This section lists some of the directives and frameworks currently in place that help protect the FA sector.

The Department of Homeland Security published the *National Infrastructure Protection Plan (NIPP) Food and Agriculture Sector-Specific Plan (SPP) for 2015*. It is a guide to improve the security and resilience of the FA Sector. The plan is a collaborative effort with the private sector and, according to the report, the sector has already taken significant steps to improve security and resilience. On the topic of cybersecurity, the plan provides general-purpose advice applicable to all industries, as follows:

> *Cyber threats and attack tools evolve rapidly as the cyberattacking community shows ingenuity. Most attacks can be blocked by continuously updated computer security programs. Such programs involve adherence to procedural safeguards for the system; an effective, continuously adaptive firewall; the application of intrusion detection and intrusion prevention systems for detecting, reporting, and preventing external threats to the network and information systems; surveillance programs for detecting insider threats; the continuous training of system users on proper security procedures; use of passwords resistant to hacker compromise; and related safeguards. Sector partners use cybersecurity measures as part of good business practices.* (DHS, 2015, p6)

Although not specific to the FA Sector, the *National Institute of Standards and Technology (NIST) Cybersecurity Framework* is a general set of standards, guidelines, and best practices for managing cybersecurity risk. The United States Computer Emergency Response Team (US-CERT) created the *Critical Infrastructure Cyber Community Voluntary Program* to help organizations use the NIST Cybersecurity Framework. It also provides cybersecurity resources to owners and operators of critical infrastructure.

In addition, *Executive Order 13636: Improving Critical Infrastructure Cybersecurity* reinforces the need for public and private entities to work together to improve the security of critical infrastructure. According to its published fact sheet (DHS, 2013), the order directs the Executive Branch to:

- Develop a technology-neutral voluntary cybersecurity framework
- Promote and incentivize the adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
- Explore the use of existing regulation to promote cyber security

Although not a comprehensive list, these frameworks and directives demonstrate the Federal Government's commitment to maintaining the security of the nation's critical infrastructure which includes, of course, the FA Sector.

Assessing Risk

The Federal government performs high-level vulnerability assessments on a variety of food and agricultural products under the regulatory authority of the FDA and USDA. (DHS, 2015, p27) From a cybersecurity perspective, they are particularly concerned with the use of Industrial Control Systems (ICS) in food production and processing plants. For example, according to the *CARVER+Shock Primer*

(FDA, p3), one of the goals of terrorist organizations is to cause mass mortality by adding toxic agents to food products. Terrorists could exploit vulnerabilities in ICS systems to achieve that goal.

The CARVER+Shock method is a tool for assessing vulnerabilities that has been adapted for the FA Sector. It encourages organizations to think like an attacker to identify vulnerabilities. CARVER is an acronym for the six attributes that help evaluate each potential target: Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability. Given that this tool is meant to help critical infrastructure, it also considers the psychological "shock" value of a successful attack, which may include health and economic impacts. (FDA, p2-3) An organization can use this tool to identify the weakest points in its infrastructure, and then use that knowledge to prioritize how to allocate resources to protect the vulnerabilities.

The DHS identified the following cybersecurity risks in their *National Infrastructure Protection Plan (NIPP) Food and Agriculture Sector-Specific Plan (SPP) for 2015*:

- Blocked or delayed flow of information through ICS networks
- Unauthorized changes to instructions, commands, or alarm thresholds that could potentially damage, disable, or shutdown equipment
- Dissemination of inaccurate information to system operators, to either disguise unauthorized changes or to initiate inappropriate actions
- Modification of ICS software or settings, or infection of ICS software with malware
- Interference with the operation of safety systems

(DHS, 2015, p.28)

Smart Farming

As the world's population continues to grow and worldwide demand for food continues to increase, farmers are increasingly turning to technology to improve their productivity and maximize yields. “Smart Farming,” also known as precision agriculture, refers to the use of advanced technology to improve productivity in the agriculture industry.

One example of smart farming is to install moisture sensors throughout a grove that take precise measurements of the condition of the soil. These sensors upload the information to a cloud-based analytics service which crunches the data. The results of the calculations are then sent to the farm’s irrigation system, which carefully applies measured amounts of water to specific plants and, when necessary, delivers appropriate doses of fertilizer. (Economist, 2016) By applying technology in such a way, farmers can dramatically increase their productivity. However, they can also make themselves vulnerable to cyber-related attacks.

As is common in today’s digital world, the high-tech software and interconnected electronic devices produced today are not always built with security in mind. Market pressures and financial constraints cause manufacturers to prioritize usability and cost over security, leaving users vulnerable (FBI, 2016, p3).

While researching this paper, I came across four categories of cyber-related vulnerabilities associated with the FA Sector and smart farming in particular. These categories are:

- Devices that measure things and produce data
- Services that analyze the data produced by electronic devices
- Robots and drones that automate tasks
- Intellectual property

In the following sections, I’ll discuss the vulnerabilities associated with each of these categories.

Smart Devices

The publication *The Economist*, in its *Technology Quarterly: The Future of Agriculture* (September 2016), provided a broad overview of the types of devices that are improving the precision of agriculture. Some examples include:

- Devices that sample soil to track properties such as mineral content and porosity
- Devices that map the contour of land, which help indicate how water moves around
- Detectors that monitor moisture levels at multiple depths
- Devices placed within animals that measure stomach acidity in order to detect digestive problems
- Sensors that detect an animal's movement and level of fitness, which can provide advance warning of physical issues. Movement detectors can also help predict when a cow is ready for insemination.

These devices are subject to the same types of cyber vulnerabilities found in smart devices developed for other industries or as consumer products in the Internet of Things (IoT). M. Ammar et al. (2017) surveyed the security of IoT frameworks and noted that vulnerabilities may exist in the following areas:

- The physical devices themselves
- The servers that route, store, and access the data produced by the devices
- End-user applications that interact with the device and access the data (p9)

The vast majority of IoT devices use commercial off the shelf (COTS) microcontrollers that aren't deployed with hardware security in mind. If a device does use encryption, the device may outlast the value of the encryption, i.e., the encryption may be rendered obsolete well before the device is retired. Finally, physical devices can be stolen or moved from their location. (p23)

When reviewing IoT frameworks, M. Ammar et al. (2017) specifically researched the following categories for security vulnerabilities:

- Authentication methods
- Authorization and access control
- Communication protocols

These categories are the responsibility of the companies that build the products and the engineers who design them. If not secured, the devices are at risk.

Data Analytics

Modern farming produces vast amounts of data—data that needs to be aggregated, analyzed, and provided back to farmers as useful information. To meet this need, companies both large and small are entering the data analytics business. These businesses provide data-based farm management services customized to the FA Sector. For example, research firms can analyze data from a variety of sources, such as smart devices and satellite data, to review the performance of a particular field over long periods of time. They can use this type of data to forecast the size of harvests before they are gathered, producing powerful financial and political information (Economist, 2016). These data-crunching services are typically cloud-based, and farmers face the same risks and vulnerabilities of any industry that shares mission-critical data with third-parties. For example, in the *Private Industry Notification* released by the FBI in March of 2016, the FBI described a specific threat to data that tracks crop availability and pricing. Criminals want to steal data that can be used to predict crop pricing, which they can then use to illegally exploit agriculture markets.

Zissis and Lekkas (2010) discussed cloud security issues and identified the following security categories:

- Trust. The cloud environment must be able to clearly identify, authenticate, authorize, and monitor who or what is accessing the data.
- Security controls. Security controls must be in place to assess risks, identify threats, and implement countermeasures.
- Data confidentiality and privacy. Cloud computing is based on model in which computing resources are shared, but data must still be kept confidential between users.
- Data integrity. Users' data must be protected from unauthorized deletion, modification, theft, or fabrication.
- Availability. Data must be accessible and usable upon demand.

Zissis and Lekkas (2010) recommend employing a trusted third party (TTP) to preserve the confidentiality, integrity, and authenticity of data and communications. The TTP can be used for all levels of authentication in the cloud infrastructure, leveraging Public Key Infrastructure (PKI) to establish secure connections.

Robots and Drones

Farmers are increasingly turning to automation to improve productivity. Robotics is developing rapidly, and control systems are getting better and cheaper every day. (Economist, 2016)

One novel and conspicuous type of robot is the unmanned aerial drone, such as a quad-copter popular with hobbyists. A typical use-case is to carry a multispectral camera over the land. This type of camera detects how strongly plants absorb or reflect different wavelengths of sunlight to determine which crops are flourishing and which are not. Drones are not limited to quad-copters; they may be flying wings or other airborne vehicles that appear similar to traditional light aircraft.

Farming robots are currently being developed that can autonomously drive around fields, identify weeds, and eliminate them without harming the crops. Other robots are being developed that can apply fertilizer to plants in individualized doses, based on information generated from a variety of sources. In addition, fruit-picking is a labor-intensive and time-consuming task that is ripe for automation. Robot pickers, armed with blades, baskets, and conveyers, may soon replace the human laborers.

The risks inherent in robotics have been well documented in contemporary Science Fiction. In addition to simply "bricking" critical equipment, one can easily imagine a hacker taking control of autonomous, heavy machinery with wheels, arms, and blades, and wreaking havoc. If done on a large scale, such an attack could be both devastating economically and absolutely terrifying to the general public. Many robots will likely be produced by large manufacturers such as John Deere and standardized throughout the sector. This uniformity means that if an attacker exploits a zero-day vulnerability, the attack may be scalable across the sector. It also stresses the importance of developing highly secure devices and the social responsibility of robot manufacturers to engineer their products with security at the forefront.

Theft of Intellectual Property

Large corporations are investing heavily in cutting-edge technologies to support the FA Sector. John Deere, for example, designs and builds advanced farming equipment. Dow and DuPont develop seeds and agricultural chemicals, along with giants such as Monsanto that also research biotechnologies such as genome editing. (Economist, 2017) Their intellectual property is vulnerable to cyber espionage. The Internet Security Alliance (2017), warns that "Foreign nations are trying to illegally get ahold of American agricultural technology, particularly data on genetic engineering, improved seeds and fertilizer as well as information related to organic insecticide and irrigation equipment."

As is common knowledge in the cyber security field, China is extremely active in cyber espionage and poses an ongoing, persistent threat to Western intellectual property. Numerous stories abound of

Chinese hackers brazenly infiltrating corporate networks and stealing valuable information—often without bothering to cover their tracks. Other countries and companies participate in cyber espionage, too, often justifying their actions as a requirement for national security or for maintaining a competitive edge. In addition, hacktivists may post a threat to companies that are developing technologies that they find immoral, such as genetic editing. Faced with such formidable threats, high-tech organizations in the FA Sector must work diligently to harden defenses and protect their intellectual property from theft or attack.

SCADA Systems

Finally, one cannot conclude a survey of the cyber security of the FA Sector without mentioning SCADA systems. As mentioned earlier, one of the goals of terrorist organizations is to cause mass mortality by adding toxic agents to food products. One potential attack vector could be through the SCADA devices used by food processing facilities. As such, the FA Sector is just as vulnerable to attacks on SCADA systems as other industries and infrastructure sectors that rely on these devices.

Conclusion

The FA Sector is a critical component of the national infrastructure. It is also closely intertwined with other critical sectors. While farmers are a fairly risk-averse bunch--they are traditionally not early adopters of cutting-edge new technology--they are under increasing pressure to increase yields as the world population demands more and more food. Farmers are turning to advanced new technologies to meet this need. However, this new technology comes with risks. Fortunately (or unfortunately?), most of the cyber risks are also shared with other critical infrastructure sectors and technology companies in general. The Federal Government recognizes the risks and is devoting significant resources to mitigate them. The fight to secure the nation’s infrastructure—and the FA Sector--is far from over. But the FA Sector is not facing these threats alone.

Sources

Department of Homeland Security. (June 12, 2013). *Executive Order 13636: Improving Critical Infrastructure Cybersecurity*.

Department of Homeland Security. (March 2013). *Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience*.

Department of Homeland Security. (2015). *National Infrastructure Protection Plan (NIPP) Food and Agriculture Sector-Specific Plan (SPP) for 2015*.

D. Zissis, D. Lekkas, (2010). *Addressing cloud security issues*. Future Generation Computer Systems 28 (2012) 583–592. Retrieved from https://doi.org/10.1016/j.future.2010.12.006

Economist. (September 2016) *Technology Quarterly: The Future of Agriculture*. Retrieved from https://www.economist.com/technology-quarterly/2016-06-09/factory-fresh

Federal Bureau of Investigation, Cyber Division. (March 31, 2016). *Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector*.

Food & Drug Administration. (September 2009). *CARVER + Shock Primer*.

Internet Security Alliance. (2017). *Cybersecurity in the Food and Agriculture Sector*. Retrieved from https://isalliance.org/sectors/agriculture/

J. Lopez et al. (Eds.): *Critical Information Infrastructure Protection*, LNCS 7130, pp. 1–14 & 39-51, 2012.

M. Ammar, G. Russello, B. Crispo. (2017) *Internet of Things: A survey on the security of IoT frameworks*. Journal of Information Security and Applications 38 (2018) 8–27. Retrieved from https://doi.org/10.1016/j.jisa.2017.11.002

United States Computer Emergency Readiness Team. *Critical Infrastructure Cyber Community Voluntary Program*. Retrieved from https://www.us-cert.gov/ccubedvp