Testimony for the Record
Submitted to the
House Agriculture Committee
Subcommittee on Livestock and Foreign Agriculture

Jennifer van de Ligt, PhD

Director, Food Protection and Defense Institute
Associate Professor, College of Veterinary Medicine
University of Minnesota

Chairman Jim Costa and Ranking Member Dusty Johnson, and Members of the Subcommittee on Livestock and Foreign Agriculture, thank you for inviting me to participate in today's hearing. It is an honor to appear before you.

I am the Director of the Food Protection and Defense Institute and Associate Professor in the College of Veterinary Medicine at the University of Minnesota.

The Food Protection and Defense Institute (FPDI) at the University of Minnesota is an Emeritus Homeland Security Center of Excellence dedicated to providing leading-edge research, technical innovation, and education to protect the food system from disruption. Since 2004, FPDI has partnered with stakeholders across government, industry, NGOs, and academia to assure product integrity, supply chain resilience, and brand protection throughout the food and agriculture sector.

I have an extensive background in food defense, animal feed and human food production, human and animal nutrition, systems modeling, and scientific and regulatory affairs, with academic, industry, and global perspective. My academic career has focused on building collaborations to assure effective public-private partnership and stakeholder engagement to advance food and feed security, safety, defense, and supply-chain resilience. Prior to joining the University of Minnesota, I held numerous leadership positions at a multinational food company operating in 70 countries where I provided nutrition, regulatory, and scientific affairs expertise across their human food and animal feed portfolios. I have more than 130 global patents and patent applications covering specialty ingredients, processing technology, packaging innovations, and biology-based dynamic modeling formulation systems.

Background

Cyber risk is not new to the food and agriculture sector, but the risk of significant business disruption and significant national security threats from cyberattack are growing.[1] Traditional information technology (IT) in the form of email, data storage, records retention, and point of sale activities are ubiquitous and have been for many years. These systems are updated regularly with most food firms relying on in-house, or third-party, IT providers to manage cybersecurity for their systems.

The newer cyber risk in the food and agriculture sector is the growing dependence upon cyber-based information and operational technology (OT) systems used to perform an ever-expanding variety of normal operating procedures. The operational technology systems, including industrial control systems and internet-connected sensors, controllers, and devices (sometimes referred to as the internet of things or IOT), manage the most critical aspects of food production, typically have the lowest level of integrated cybersecurity protections, and are often not included in enterprise cybersecurity plans, protections, and training.

Two pieces of operational technology illuminate aspects of cyber risk in the food and agriculture sector. First, a pasteurizer in a fluid milk or juice manufacturing facility is critical to assuring the food safety of those products. The pasteurization time and temperature are controlled by sensors communicating with control systems monitored remotely by food safety professionals. Second, in beef harvest facilities, carcasses must be split into right and left halves prior to further processing. This splitting is increasingly being done by robotic carcass splitters. If either of these pieces of equipment are compromised through a cyberattack, the facility would be required to shut down and

[1] Food Protection and Defense Institute. 2019. Adulterating More Than Food: The Cyber Risk to Food Processing and Manufacturing. https://hdl.handle.net/11299/217703

economic consequences would result. Depending upon the type of cyberattack and the speed at which it is detected, other consequences may also occur. For example, if the pasteurizer is compromised, it may inaccurately, and possibly even maliciously, report and record that acceptable food safety metrics were reached – even though they were not – resulting in unsafe product being distributed and wide-scale human health harm. Cyberattack on the carcass splitter could result in serious worker injury to human operators present in those areas.

Although the above examples are hypothetical and used to illustrate types of technology at risk of cyberattack, the concept of cyberattack in the food and agriculture sector is not hypothetical. It has been occurring for years and is gaining recognition as a significant threat to business continuity and national security. In fact, Dragos, Inc. reported that ransomware attacks on industrial entities increased more than 500% from 2018 to 2020.[2]

History of cyber-attacks in the food and agriculture infrastructure

As early as 1998, cyber criminals targeted the food and agriculture sector with denial-of-service attacks, ecommerce thefts, and intellectual property thefts. However, most of these attacks had limited public exposure to avoid brand damage. The more recent cyberattacks have evolved to compromise networks, disrupt operations, and/or exfiltrate vast amounts of data. The scale of these recent attacks, in terms of ransoms paid and levels of operational disruption due to the significant consolidation across the sector, make such events difficult to keep from the public eye. To make matters worse, the rise of cryptocurrency payments to end the attack and recover data makes it exceptionally hard for law enforcement to identify the criminal organization and track and recover payments.

Since late 2020, major cyber incidents (e.g., SolarWinds, E&J Gallo, Molson Coors, Colonial Pipeline, JBS, Kaseya, and others) have severely disrupted the ability to conduct business for many companies in the food and agriculture sector. With many of these companies paying ransom to end the attack, it is likely that attacks will continue. In addition, the pandemic highlighted how food and agriculture sector consolidation and interdependencies increase not only risk of disruption but also the probability that accompanying publicity will result in increased targeting of food and agriculture sector infrastructure. Ransomware, data theft, and operational disruption are not the only issue. As shown with water treatment facilities in California and Florida, cyberattacks are also intended to harm health. In these attacks, water disinfection chemical levels were adjusted to harmful levels.

Implications of the growing cyber risk in the food and agriculture sector

The food and agriculture sector is incredibly diverse. It is composed of facilities ranging from small businesses and family farms to multinational corporations that produce an infinite variety of foods. Some aspects of the food and agriculture sector are highly distributed, while some are highly consolidated. Each and every business, farm, production facility, and company is individually vulnerable to cyberattack. On a broader scale, however, the food system is one of the most interconnected and interdependent systems within the critical infrastructures. Relationships among food companies can include supplier, customer, and competitor simultaneously. These interconnections often mean that data flows routinely and fluidly across the sector. From a cyber perspective, this amplifies the attack surface and the risk. It also amplifies the potential magnitude of system disruption and failure from a cyberattack, including its secondary and tertiary cascading impacts.

---

[2] Larson and Singleton. 2020. Ransomware in ICS Environments.

The food and agriculture sector is labor intensive. However, a history of labor shortages coupled with technology advancements have driven automation in the sector. The changing worker health provisions and expectations exacerbated by labor shortages during the pandemic have only accelerated the motivation within the food and agriculture sector to increase automation. However, with every advancement comes unintended consequences. With increased automation and the concomitant rise in computational and network complexity, cyber risk also increases.

Regardless of why cyber risk exists, cyberattacks have the potential to cause catastrophic disruption and endanger national security concerns. For example, the recent JBS cyberattack disrupted meat processing operations in several countries and simultaneously caused disruptions to supply chains, logistics, and transportation to customers. And it increased consumer prices. This amplification of disruption can easily result in national security threats depending upon the scale of attack and subsequent disruption.

As a hypothetical example of a national security threat, consider for a moment the impact if both of the only two HDPE pellet plants that produce the gallon milk jug preforms were the victims of a simultaneous cyberattack? We know that during Hurricane Katrina when just one of these HDPE facilities was compromised, the supply of fluid milk at the consumer level plummeted to shortage levels in many areas of the country while dairy farmers dumped millions of gallons of milk. A situation, such as this, could be repeated and affect a broad area of the nation in the event of a targeted cyberattack.

Our FPDI research and experience engaging with food system stakeholders led us to identify the following primary (but not exclusive) causes for cybersecurity risk to agricultural and food products supply chains:

- Lack of awareness throughout the sector of the scale of cybersecurity risks to agricultural and food processing and manufacturing and the potential consequences if those risks were realized.
- Lack of regulatory guidance and clarity regarding how cybersecurity risks should be accounted for and addressed in assessing food safety risks.
- Lack of standards for the cybersecurity of agricultural and food processing systems, both for the operation of those systems and for the design and development of the software and hardware that comprise them.
- Lack of research and vulnerability assessment data upon which to make evidence-based cybersecurity risk mitigation and policymaking decisions. This especially hampers the ability to prioritize the most vulnerable products or processes for mitigation efforts.
- Lack of cybersecurity education and training among operations technology personnel and lack of control systems knowledge among information technology personnel tasked with cybersecurity at agriculture and food companies. This is particularly acute at small- and medium-sized businesses.

It should also be recognized that although some food and agriculture sector partners may recognize the risk, constraints exist in their ability to manage that risk. They must balance a multitude of supply chain, food safety, labor, financial, and other operational risks in addition to cyber risk. Not only does managing cyber risk increase operational costs, but there are also very few experts with the knowledge and experience to effectively enhance cybersecurity in the food and agriculture operational environment. This type of expert is often recognized as irreplaceable and are sometimes referred to as 'unicorns' within the food industry. We need to train and field many more of them.

Recommendations for enhanced cyber resilience

Current federal law (the Food Safety Modernization Act) specifies that covered facilities must establish and implement a food safety system that includes an analysis of hazards and risk-based preventive controls. Regulations promulgated by FDA require a written food safety plan that includes steps for hazard analysis, preventive controls, oversight and management of preventive controls, monitoring, corrective actions, and verification. Few of these steps can be undertaken without information technology, industrial control systems, and internet-based communication systems. Any compromise of these supporting systems jeopardizes implementation of these critical food safety procedures, including the process controls that must be addressed in hazard analysis and protective strategies, as well as others such as product testing and environmental monitoring. In addition, more historical FDA regulations address electronic records creation, accuracy, and retention. However, aspects of the food and agriculture sector may not be covered by these regulations (e.g., USDA-regulated food facilities, farm-level production, etc.) and none of the current regulations address cybersecurity of the systems required to acquire, manage, and preserve these records.

As provided in the FPDI comments offered in response to "Notice: Supply Chains for the Production of Agricultural Commodities and Food Products, Request for Public Comments", I, as Director of FPDI, recommend the following actions:

- USDA should take the lead in developing new minimum information technology risk reduction regulations and develop new Good Manufacturing Practices (GMPs) specific to the production agriculture and food and beverage industries. These could be developed as a new set of cyber preventive controls to be consistent with the implementation of other Food Safety Modernization Act (FSMA) requirements. This action should be taken in concert with industry, the Department of Homeland Security (DHS), the Food and Drug Administration (FDA), and the Federal Bureau of Investigation (FBI).
- USDA, in collaboration with FDA, should develop sector-specific system risk reduction measures, facility-level cybersecurity risk reduction plans, and operator guidelines and training. They should also develop specific preventive controls training and reporting for cyber systems within the food and agriculture sector.
- USDA should host a series of cybersecurity review and technology forums or similar events for food and agriculture sector senior management to accelerate the education of senior leadership within industry. Senior leadership needs a better understanding of the cyber risks and the importance of investing in risk reduction for cyber systems, especially in the food and agriculture operating environment. This action should occur in partnership with the insurance industry, the cybersecurity industry, FDA, FBI, and DHS,
- USDA should develop a university-based food and agriculture sector focused cyber Center of Excellence to conduct research and education that aids in cyber risk reduction.
- USDA should collaborate with industry and DHS to establish an Information Sharing and Analysis Center (ISAC). The mission of this ISAC should be to understand evolving food and agriculture sector cyber risks as they may impact both individual facilities and entire supply chains, anticipate local and broad supply chain exposures, and monitor cyber technology shifts and emerging cyber-based or control technology risks across all aspects of the food system.

Closing Remarks

Securing the vast cyberinfrastructure and electronic information systems sustaining America's food and agriculture supply system is vital to the economic vitality of the system and our nutritional and

national security. If we do not act, we risk the nation's ability to provide a sufficiency of nutrition, the very essence of well-being for our friends, family, colleagues, constituents and institutions.

I, and the Food Protection and Defense Institute, appreciate the opportunity to engage in and contribute to this national discussion of our food system's resilience.

Thank you. I look forward to further discussion on this important topic.