Report reveals growing threat of cyberattacks to food safety

11 September 2019

Credit: University of Minnesota

A new report by University of Minnesota researchers indicates cyberattacks pose a rising threat to food production and safety.

"Adulterating More Than Food: The Cyber Risk to Food Processing and Manufacturing," released today by the University's Food Protection and Defense Institute (FPDI), illustrates the mounting cybersecurity risk facing the food industry and provides industry-specific guidance to keep operations safe and secure. The potential consequences of an attack on the industrial control systems used in the food industry include contaminated food that threatens public health, physical harm to workers, destroyed equipment, environmental damage, and massive financial losses for companies.

While cybersecurity is rarely recognized as a food safety issue, the systems companies use for processing and manufacturing food contain many vulnerabilities that experts believe will soon present a more appealing target for cyberattacks than industries that are more commonly affected by, and therefore better prepared for, such attacks.

"The food industry has not been a target of costly cyberattacks like financial, energy, and health care companies have," said Stephen Streng, lead author on the report. "However, as companies in those sectors learn to harden their defenses, the attackers will begin looking for easier victims. This report can help food companies learn about what could be coming their way and how to begin protecting themselves."

Researchers and manufacturers identified more than 200 industrial control system vulnerabilities in 2011, the report notes, with the number increasing each year through 2016, the end of the study period. The vulnerabilities are present in a wide variety of components from different vendors, making them difficult for companies to avoid. Many systems were designed before cybersecurity was a concern and use outdated operating systems and hard-coded passwords that allow attackers easier access to the system.

In addition to vulnerabilities in the systems themselves, many other factors contribute to the heightened risk of cyberattacks. Companies often lack knowledge about how their industrial control systems and IT systems interact and lack awareness about cyber risks and threats. Further, there is poor coordination and information-sharing among food system stakeholders. Meanwhile, the tools required to carry out a cyberattack are becoming more powerful and requiring less skill to use.

"The food industry has some characteristics that make it uniquely vulnerable to cyberattacks on its processing and manufacturing systems," Streng said. "Luckily, there's still time for companies to protect themselves."

Moving forward, the report recommends that the food industry foster stronger communications between operations technology and information technology (IT) staff, conduct risk assessments that

include inventories of both industrial control and IT systems, involve staff with cybersecurity expertise in procuring and deploying new industrial control systems, and extend the existing culture of food safety and defense to include cybersecurity.

"Cyberattacks could have financially devastating consequences for the food industry, particularly among smaller companies, and in the worst case can threaten the public's health," said Amy Kircher, DrPH, director of FPDI. "We hope this report will raise awareness among food industry executives of this potentially severe risk and will inspire them to start addressing it with the same care and urgency they apply to other aspects of food safety."

FPDI, a Homeland Security Center of Excellence, protects the global food supply through research, education, and the delivery of innovative solutions, addressing vulnerabilities that could lead to catastrophic damage to public health or the economy. The institute collaborates with industry, government agencies, nongovernmental organizations, and academic stakeholders to help assure product integrity, supply chain resiliency, and brand protection throughout the food system.

More information: The report is available online: foodprotection.umn.edu/research/food-cybersecurity

Food Protection and Defense Institute: foodprotection.umn.edu.

Provided by University of Minnesota