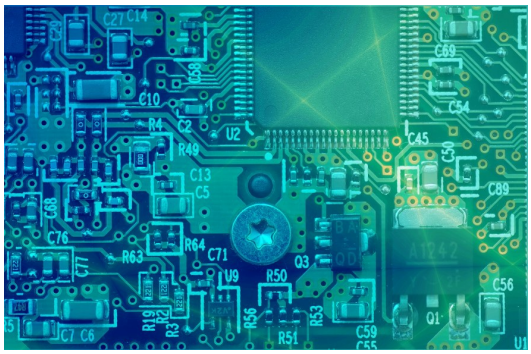
ASIAFRUIT

For fresh fruit and vegetable marketing and distribution in Asia

By Fred Searle

Wednesday 18th September 2019, 16:50 GMT



# Cyber attack risk 'growing' in food supply chains

## New report warns that as other sectors become more resilient to attack, criminals are more likely to target food industry's vulnerable systems

Global food supply chains are increasingly vulnerable to cyber attacks that could pose a risk to public health, a new report has warned.

Contaminated food, physical harm to workers, destroyed equipment, environmental damage and huge financial losses for food companies are among the potential consequences outlined in the study by the Food Protection and Defense Institute at the University of Minnesota.

Experts warn that the Industrial Control Systems (ICSs) that firms use to process and manufacture food have many vulnerabilities that are easy to exploit and will become an increasingly attractive target for criminals.

"As the energy, financial, and healthcare sectors harden their defenses in response to attacks, it's safe to assume criminals and other threat actors will move on to lower hanging fruit," the report reads.

"This could well be the food industry, which continues to use vulnerable ICSs [that are discoverable on the internet."

The study adds that operations technology (OT) staff in the food industry tend to be experts in food safety and production, but not in cybersecurity, which overwhelms most of them. "OT personnel aren't trained to develop a mindset to suspect and detect hacks if something out of the ordinary happens," the report points out.

Other factors that add to the cyber threat faced by the food industry are: a lack of knowledge about how ICSs and IT systems interact; the dependence on outsourced technology management by small- and mid-size companies; company leaders' lack of awareness regarding cyber risks and threats; and poor coordination and information sharing between companies and government agencies.

Dave Weinstein, the CSO of US cybersecurity software firm Claroty, commented: "While it doesn't receive many headlines, the cyber risk to the food and beverage manufacturing process is a serious one.

"Not only are most of the industrial control systems behind the manufacturing process inherently insecure, but many companies in this industry are embracing aggressive digital transformation initiatives.

"These efforts are great for productivity and efficiency, but they also introduce more connectivity to the manufacturing network, thus subjecting it to both commodity malware from the IT network and targeted threats."

To guard against the cyber threat, the report recommends that food companies foster more communication between their OT and IT staff; begin conducting risk assessments that include making an inventory of ICSs and IT systems; and create a culture of cybersecurity as well as food safety.