Meat Packaging Company

Cyber Attack Case Study

Buist installed Direct Digital Controls (DDC) on all refrigeration systems throughout a local meat packaging facility to provide remote control and alarming systems via the owner's IP network.

Facility:

A 30,000 sq.ft. wholesale meat packing plant with 19,000 sq.ft. of refrigerated space served by (21) individual refrigeration systems. The facility processes 200-300 pigs per day into 50,000 lbs. of wholesale packaged meat.

Process:

Every day, pigs are delivered and processed through this facility. One of the key stages at this facility, is the cooling process. The pigs are cooled from 100°F to 37°F over a 6-hour period. Meat must be held below temperature limits at all points during this process, this is monitored by the USDA to protect against bacterial contamination. Failure to maintain temperature would result in spoiled product and production losses. Each night there is more than $100,000 worth of raw meat being cooled for processing the next day.

Event:

Almost immediately upon startup, the DDC experienced catastrophic failure requiring a hard power cycle to recover. The controller resource manager showed the central processing unit was maxed out at 100% usage, meanwhile system operations at the supervisory level were halted. These failure of events put the product being held at risk because the critical function of defrost was inoperable during the event. The DDC manufacturers tech support was not able to determine the root cause, however a cyber attack was suspected. We enabled the Denial of Service (DOS) protection feature on the system per their recommendation. They also validated the system wiring and programming, but the failures continued regularly. As the war in Ukraine drew near, media chatter speculating cyber attacks from Russia made headlines. This helped us finally convince the owner to put his public facing IP port behind a VPN firewall. Once the VPN was established the problems ceased immediately. We asked the IT vendor to check the port activity logs and they found tens of thousands of random visits per second. Although the system was never hacked, the excessive traffic hits to the NIC card effectively stopped the controller from operating. It was an inconvenient and expensive learning experience. Fortunately, no product or production was lost and we maintained the customers confidence throughout the series of events.

Conclusion:

Never allow a system we service or install to be exposed to the internet without proper firewall protection. Doing so could compromise the owner's network while simultaneously risking profit loss. From this point forward we will strongly encourage the use of VPN firewalls for all remote access. We are considering requiring a liability release form to be signed by the owner before connecting an unprotected system to a public facing IP port that can be accessed worldwide. We strongly consider options like eWON or Tosibox systems if the owner does not have an IT support department.

April 2022