Cyber Security – A Real Life Story

USA Outlook Conference
December 6-7, 2021

Greg Beck, Senior Vice President
CGB Enterprises, Inc.

About CGB

- Grain Buying Handling and Transportation.
- Basic ag, rural locations, low cost model.
- Mid sized, 2500 employees.
- Had an IT plan.

What happened

- June 2020, ransomware attack near 2AM.
- 5 AM most scales inoperable.
- 7 AM, IT implemented system wide shutdown.
- Could not dump trucks, print checks, etc.
- Most computers infected.
- PLCs. Were they infected, could we operate?
- IT could “see” someone looking at us.
- Culprit was an unused PC, but still connected.

Recovery Weeks 1 - 2

- Resorted to manual everything.
  - Could not contact customers, no call lists.
  - We had no on-site scale tickets or checks.
  - Alerted state and fed licensing/warehouse office.
- Hired Stroz Friedberg and Breach Legal Counsel.
- All computers unplugged, still, we saw pinging….

Recovery

- **Weeks 3-6**
  - Ordered 344 new PCs/Laptops
  - Scale by scale IT rebuilding
  - Restored systems from backups
- **Weeks 7- 9**
  - All new protocol
  - Getting back to somewhat normal operations.
  - Still some employees w/o computers.

Outcomes

- Extremely distracting – CEO to hourly.
- Daily Exec Mgmt briefings/planning.
- Extremely time consuming.
- Expensive.
- In hindsight,
  - insisted employee failed Phishing tests had consequneces, privileges suspended.

Lessons Learned

- Executive Mgmt must take as seriously as safety or any other serious business risk.
- Be diligent on all IT phishing, spyware tests and training – AND FOLLOW UP.
- IT perform continuous risk assesments.
- Never used old PCs for scales, cameras, PLCs.

Lessons Learned, part 2

- Have a handle on where your sensitive customer data is kept and system access.
  - Paper contract balances and customer contact info.
- Train on manual procedures.
- Have back up/manual scale tickets and checks.
- Separate physical operations PLCs from network.

CONSOLIDATED GRAIN AND BARGE CO.

Thanks for listening