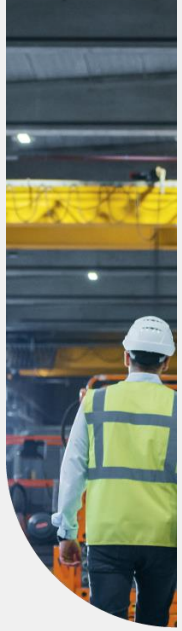


FORTINET

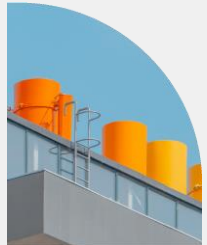
OPERATIONAL TECHNOLOGY SYMPOSIUM 2021

Operational Resilience

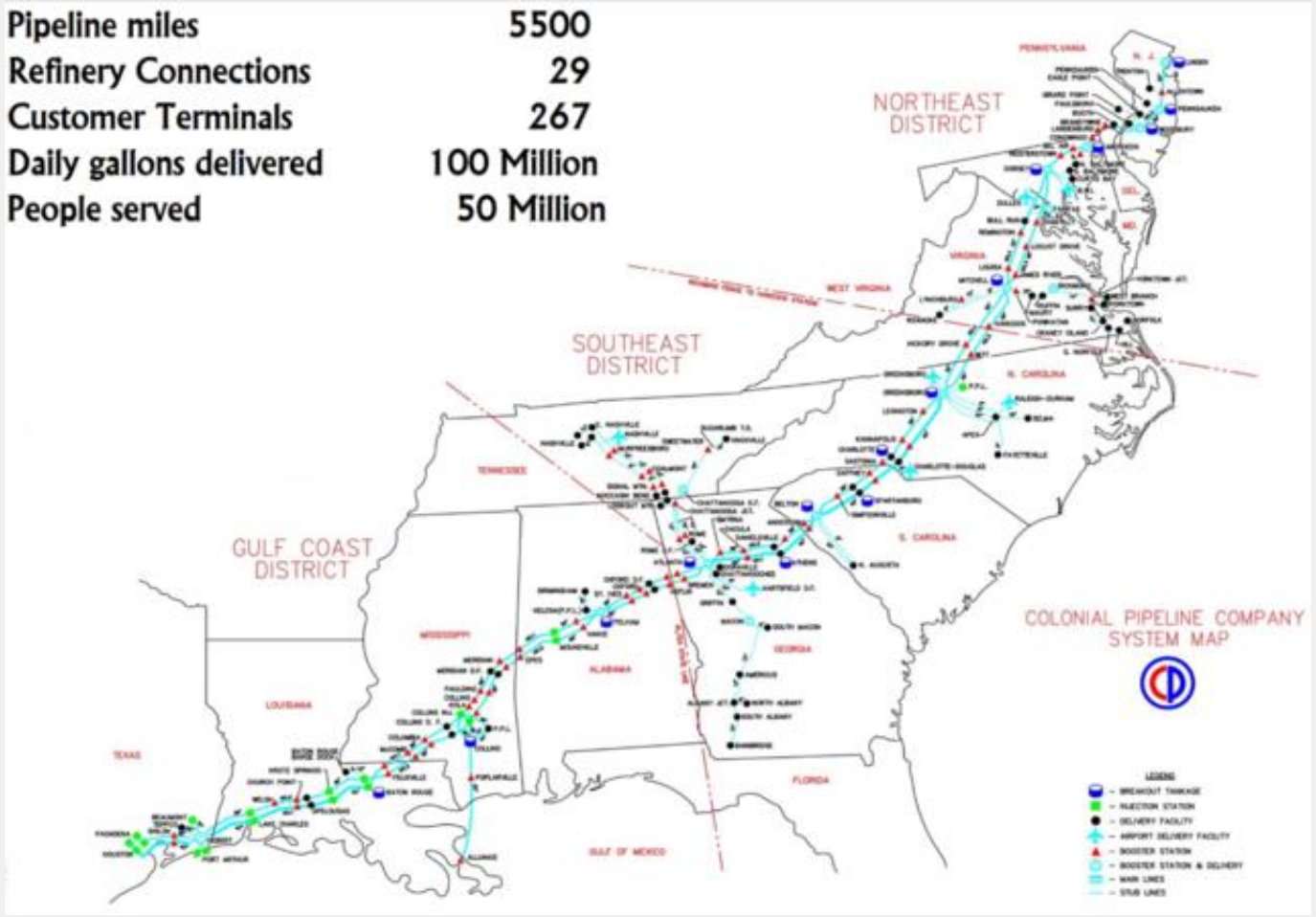
In The Face Of An Increasing Cyber Threat

Dale Peterson

Twitter: @digitalbond Web: dale-peterson.com



Colonial Pipeline Outage Due To Ransomware



What should we learn from this attack?

- Always use 2-factor authentication for remote access?
- We need more cybersecurity regulation on pipeline operators to insure a minimum set of security controls?
- Paying ransomware should be illegal?

OPERATIONAL TECHNOLOGY
SYMPOSIUM 2021

Can You Manufacture & Deliver Product If The IT Network Is Compromised?

OPERATIONAL TECHNOLOGY
SYMPOSIUM 2021

Do You Have A Recovery Time Objective (RTO)?

Are You Confident You Can Achieve It?

Risk = Consequence x Likelihood

Understand Your Organization’s Risk Management

OT consequences should be added to the risk matrix.

Accepting risk when you do not have the authority can be a career limiting decision.

Is A Power Plant Outage A High Consequence Event?

It depends …

Maui --- YES

Eastern US --- Perhaps no

When does a manufacturing plant outage become a high consequence event?

Risk = Consequence x Likelihood

Risk = Consequence x Likelihood

Consequence Reduction Story … Manufacturing

Glass factory or anything at extremely high heat.

Motion

Triton

Separating safety from control would have prevented the possibility of BOOM

Identify High Consequence Events

- These are not cyber events
- Look at your risk matrix
  - Loss of Life, Financial, Customer Impact, Environmental, Reputation …
- Identify High Consequence Events (HCE)
- Could a cyber or cyber/physical incident cause the HCE?
  - Assume a motivated and skilled attacker with admin access on the ICS

Consequence Reduction Methodologies

- Cyber PHA
- INL's Consequence-Driven, Cyber Informed Engineering (CCE)

- or -

- Keep it simple

1. Identify your HCE that could be caused by a cyber attack
2. Find a way to reduce the consequence if that cyber attack occurs. Examples: non-cyber mitigations to prevent consequence, faster recovery, alternate sources, putting people in the loop, insurance, etc.

OPERATIONAL TECHNOLOGY
SYMPOSIUM 2021

Q&A

Thank you.

Dale Peterson

OPERATIONAL TECHNOLOGY SYMPOSIUM 2021