FEAR, UNCERTAINTY, AND DOUBT

With Cybersecurity

Nathanael.Palmatier@bhcconsultants.com
Victor.Perez@bhcconsultants.com

WE WILL TALK ABOUT:

- Fear, Uncertainty and Doubt (FUD)
- FUD affects Cybersecurity
- Technology FUD in Cybersecurity
- Mitigations
- Oldsmar, Florida
- What to do?
- Network Design Suggestions

PEOPLE

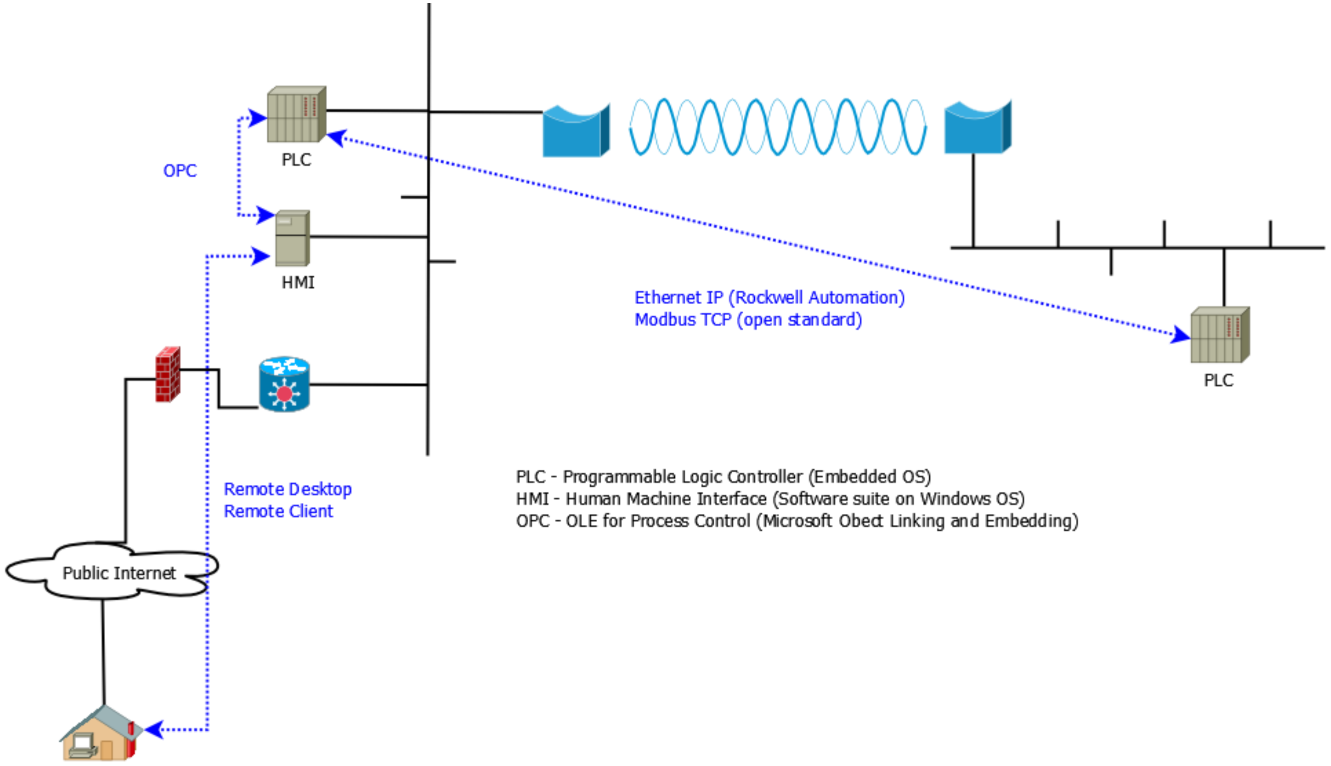
- Fear, Uncertainty, and Doubt are the most motivating factors to change behavior
- FUD used to trick people
  - Attackers, grifters, confidence manipulators
  - Trust associated with official looking or sounding
- Cybersecurity
  - Just another avenue
  - Not well understood
- Survey about Risk and Resiliency Assessments
  - 52% made or are making changes in response to Cybersecurity
  - 64% increased awareness about Cybersecurity

TECHNOLOGY ATTACKS

- Vulnerabilities in systems
  - Computer Programmers would need to code everything perfectly
  - Every code library also requires perfection
  - Most code is programmed to work, not to perfection
- Attacks always get better – Bruce Schneier
  - Analogous to computer security even though Mr. Schneier said in context of Cryptography
  - Cryptography, Computer Science, Software Engineering, Applied Mathematics, et cetra are realated
- Faustian Bargain
  - Static systems will be at risk
  - System changes can cause vulnerabilities

TECHNOLOGY UNCERTAINTY

- Beware of jargon
  - ICS – Industrial Control System
  - SecOps, DevOps, OT, IT
- Example: Zero trust
  - Philosophy; unbreakable and unfalsifiable
  - Is not a single product or service
- IT tools may not be appropriate for ICS
  - Anti-virus or Remote Desktop on a PLC?



PLC - Programmable Logic Controller (Embedded OS)
HMI - Human Machine Interface (Software suite on Windows OS)
OPC - OLE for Process Control (Microsoft Obect Linking and Embedding)

TECHNOLOGY DOUBTS

Internet Downside

- Remote attacks
- Constant updating
- Insurance
- Speed of change

Internet Upside

- Remote access
- Information collection
- Access to help
- Speed of information

ATTACKS AND FRIENDS

- Most attacks use same vulnerabilities
  - Email phishing, vishing, smishing, spear phishing
- Prado distribution – Assume 80% of attacks from 20% of vulnerabilities
  - Reality more concentrated, almost all attacks involve top 10 vulnerabilities
- Most attacks will be general
  - Network scans or other passive
  - Wide-area spray (i.e., shotgun)
  - Not specific to you

- Types of Attacks
  - Weak or compromised passwords
  - Malware via email, browser, other
  - Man-in-the-Middle Attacks
  - Denial-of-Service
  - Zero-day Exploits
  - Vulnerable embedded systems or network appliances

MITIGATION

- Plan ahead
  - Prepare for bad-case scenarios
  - Everyone has a plan before they get punched in the nose – Mike Tyson
  - Table-Top exercises
- Learn from other people
  - Their experiences
  - And their mistakes so you don't have to make the same ones
- What can you control and influence?

TABLETOP EXERCISES

- Like haircuts, how bad can it get?
  - What is important?
  - What can wait?
- Practice the response
  - Know who to contact?
  - What to do?
- Practice at recovering a bad to worst case scenario
  - Real life should not be worse
  -

OLDSMAR, FLORIDA – FEBRUARY 5TH, 2020

- "Dangerous Stuff: Hackers Tried to Poison Florida Town"
  – NY Times Feb 8th
- "Florida facility hack used a dormant remote access software, sheriff says"
  – CNN Feb 10th
- Widespread coverage
  - Operator noticed unusual activity and responded well
  - Attention grabbing, near-miss
- Not much damage, lots of noise

OLDSMAR, FLORIDA – FEBRUARY 5TH, 2020

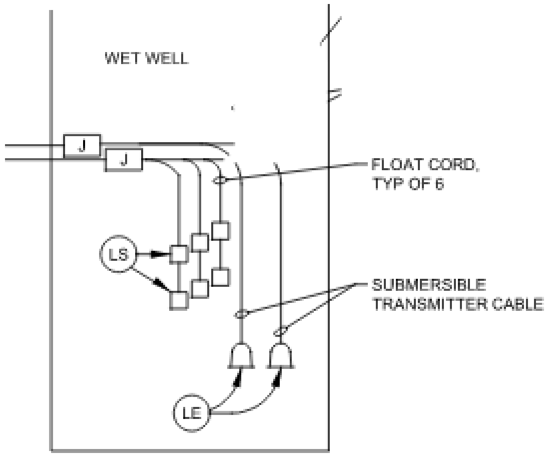
- FBI, CISA, EPA, MS-ISAC offered general recommendations
  - Use latest Operating System software (Windows 11)
  - Use Multi-factor authentication
  - Use strong passwords
  - Update anti-virus, spam filters, and firewalls
  - Audit Network Configurations
  - Audit network for unused RDP endpoints
  - Audit [system and network] logs for all remote connection attempts
  - Train Users to identify and report social engineering
  - Identify and suspend access of users exhibiting suspicious activity
- Good for ICS, Office Computers, Home Computers, Friends and Family

OLDSMAR, FLORIDA – FEBRUARY 5TH, 2020

- FBI, CISA, EPA, MS-ISAC offered Water and Wastewater recommendations
- Install Cyber-physical safety systems
  - Arrange backup systems independent of network accessible systems
  - Examples:
    - Pump-down float switch backup system
    - Pressure switch backup system
    - Standalone controllers
    - Limit storage of harmful substances

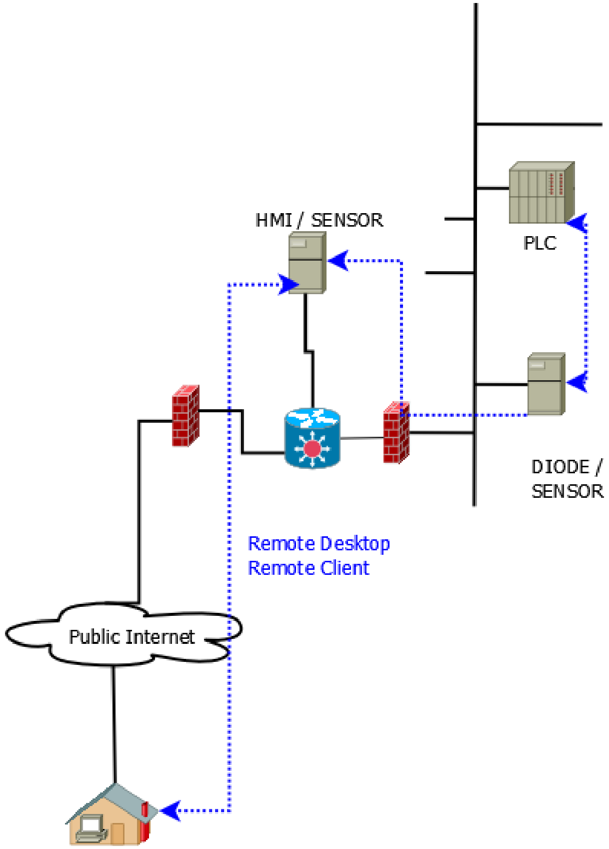
CYBER-PHYSICAL SAFETY SYSTEMS

- Complexity in systems
  - Optimizing may require complexity
  - Ideally add Internet with same risk
  - Fail safe, limp-home, backup
- Separate Monitoring, Alarming, and Control
  - Monitor Alarm and Control
  - Alarm on Control or Monitoring Problems
- Build into system design
  - Cybersecurity



CYBER-PHYSICAL SAFETY SYSTEMS

- Segment and monitor ICS
  - DMZ/Frontend analog
  - Restrict movement on ICS
- Sensor and monitoring
  - Remote access attempts
  - Unusual activity
  - Monitor and Alarm network



WHAT WE SPOKE ABOUT:

- Fear, Uncertainty and Doubt (FUD)
- FUD affects Cybersecurity
- Technology FUD in Cybersecurity
- Mitigations
- Oldsmar, Florida
- What to do?
- Network Design Suggestions

THANK YOUS

- Contacts
- Victor Perez-Bonilla
  victor.perez@bhcconsultants.com
- Nathanael Palmatier
  nathanael.palmatier@bhcconsultants.com

- Thanks to:
  - Margarita Rodriguez, BHC
  - Venu Kandiah, Xylem
  - Tait Covert, Seattle Computing
  - James Cross, Quality Controls Corporation

INCREMENTAL IMPROVEMENT WITH PUBLIC WORKS

- Great Stink of London – 1858
  - Limestone treatment – didn't work
  - 95°F summer day
  - Parliament couldn't conduct business
  - August 1858 Parliament organized wastewater collection (design TBD)
- Sinking of Princess Alice – 1878
  - Between 600-700 passengers and crew drowned
  - Many deaths attributed to raw sewage in River Thames
- Ministry of Public Building and Works – Crossness and Beckton – 1880s