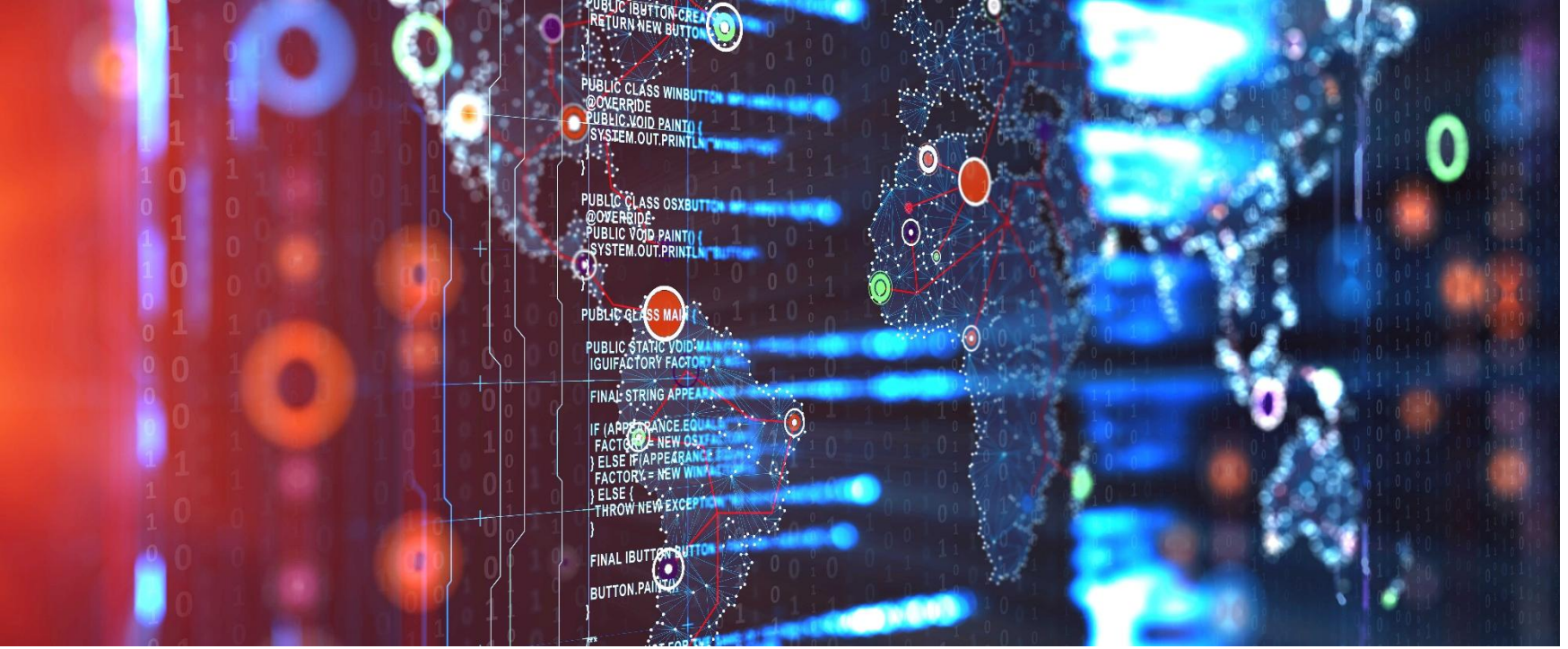



# Near Miss? Implications of the Florida Water Utility Cyberattack

March 9, 2021

*This presentation may contain photos taken prior to COVID-19 pandemic*

# GOALS

1. Update on Oldsmar Water Treatment Plant Cyber Incident
    1. What do we know about the incident?
    2. What are common mitigations that would have helped?
2. What are the common challenges for utilities to combat cyber threats?
3. Review Common Mitigations and Best Practices

# Presenters

**David Brearley, GICSP, PMP**

Operational Technology
Cybersecurity Director

*David.Brearley@hdrinc.com*

**Jim Schultz, P.E., CISSP, GICSP, CCNA, C|EH**

Cybersecurity Network Engineer

*James.Schultz@hdrinc.com*

# AGENDA

01 Oldsmar WTP Cyber Attack

02 Common Challenges

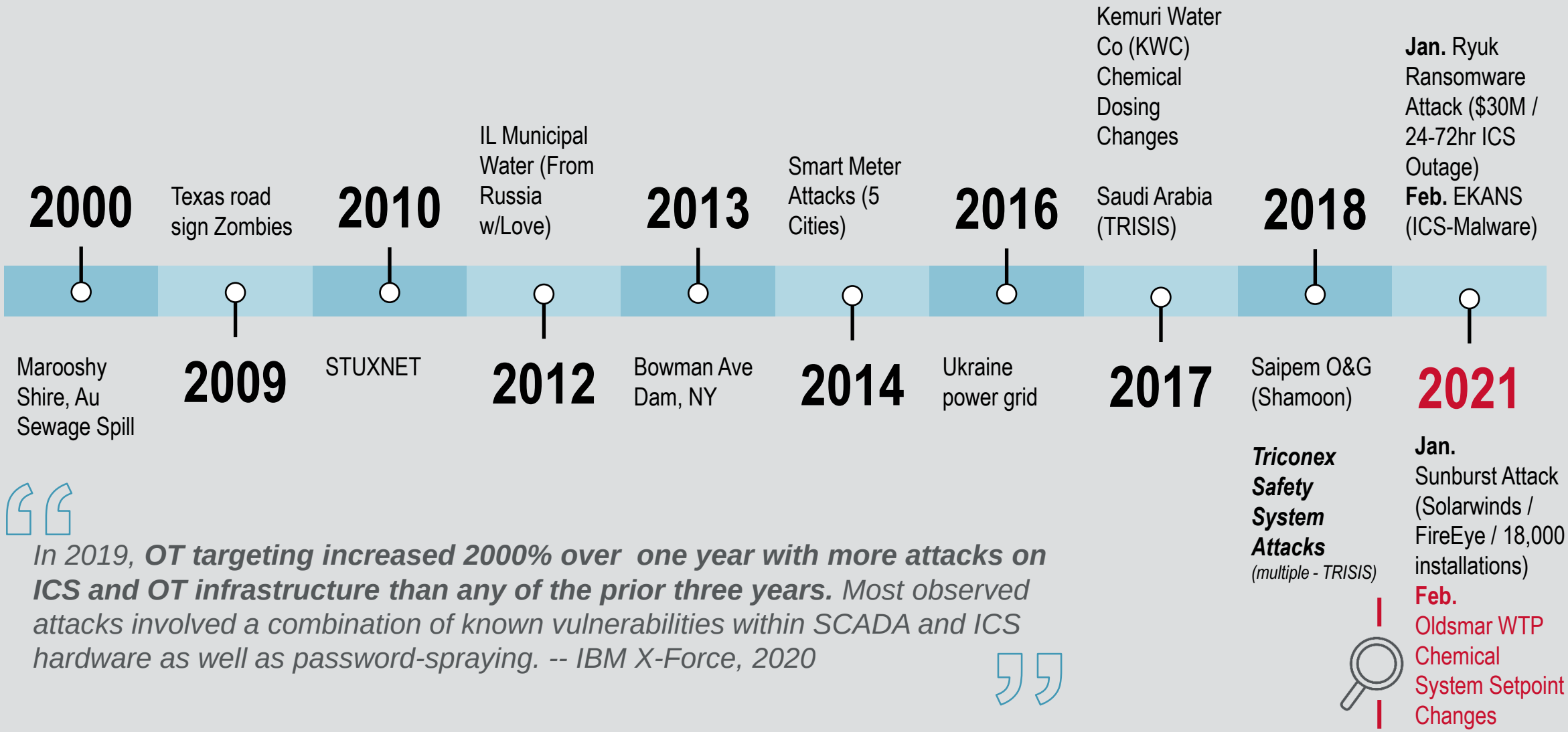
03 Cybersecurity Mitigations

04 Q&A / FAQs

01

# Oldsmar WTP Cyber Attack (2021-02-08)

# Successful Attacks




*In 2019, **OT targeting increased 2000% over one year with more attacks on ICS and OT infrastructure than any of the prior three years.** Most observed attacks involved a combination of known vulnerabilities within SCADA and ICS hardware as well as password-spraying. -- IBM X-Force, 2020*

# Oldsmar WTP Incident (Feb 8, 2021)

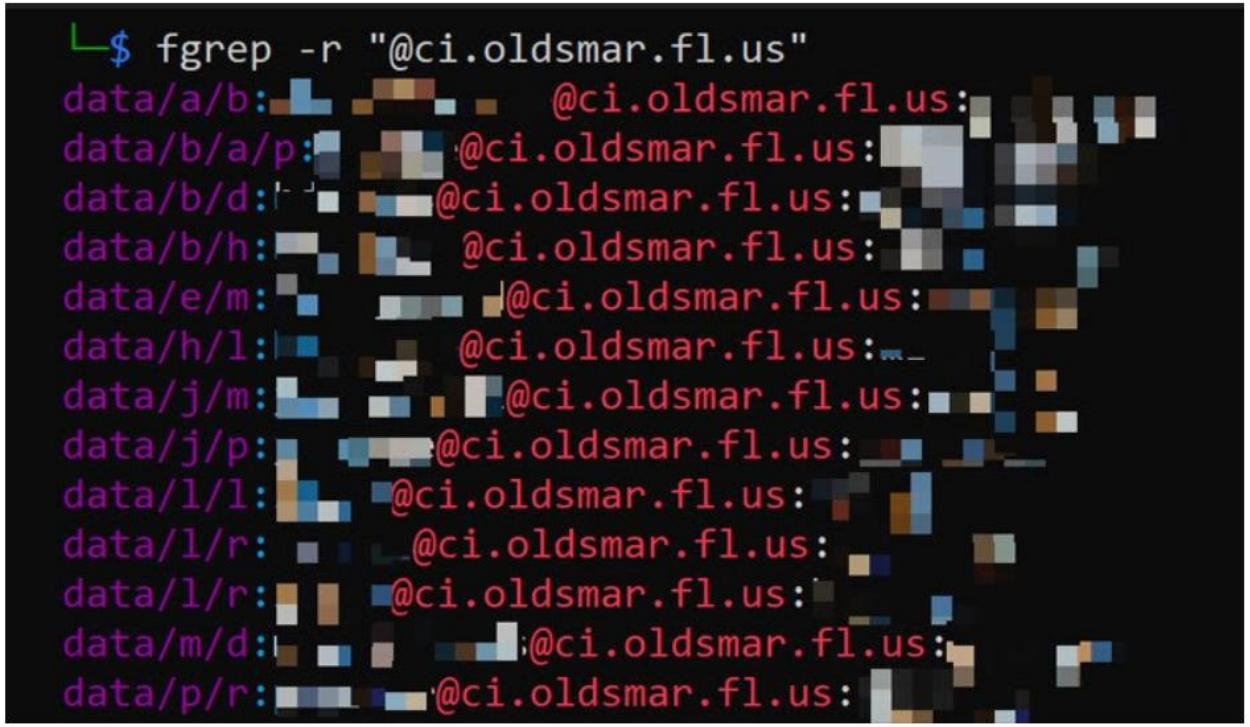
## Who?

- Attacker – outside source unknown
- Owner: Oldsmar, FL WTP

## What?

- Access via remote monitoring and control application
- Adversary changed chemical setpoints
- Accessed systems at least <u>twice</u>

On Tuesday, February 2, the largest compilation of breached usernames and passwords, known as COMB, was leaked online. COMB contains 3.2 billion unique email/password pairs. As we recently discovered, this includes the credentials for the Oldsmar water plant in Florida.




Three days after COMB was leaked, an unknown attacker entered Oldsmar's computer systems and attempted to poison the water supply by increasing lye levels 100 times.

Source: https://cybernews.com/news/oldsmar-florida-water-facility-credentials-contained-in-comb-data-leak/

*The biggest problem is that most people don't think there is a problem*

# Oldsmar WTP Incident (Feb 8, 2021)

## How?

- Created **Remote Desktop** Session using TeamViewer
- No **setpoint validation** in PLC or HMI
- Obsolete operating systems, **no firewall**, direct internet connection
- Poor credential **(user/password)** management
- Roles, Responsibilities, Procedures and Communications issues

## Indicators?

- **Mouse movement** on screen
- Setpoint modification – caught only be operator rounds (due to significant setpoint modification)
- Attacker logged in **twice in one day**
- More to come as investigation continues…

**It could have been much, much worse… why did attacker show their hand so quickly?**

02

# Common Challenges

**You have to be right 100% of the time, the cyber criminals only have to be right once!**

# Common Challenges

- **Recognition of Cyber as a potential risk (undefined risk tolerance)**
- Lacking System Maintenance
- Controls Staff
  - Lacking cybersecurity skillset
  - Inadequate number of staff to both maintain and monitor for threats
  - No controls or IT staff for support
- Inaccurate, Incomplete or Missing Documentation

# Cost of Cybersecurity Mitigations

- Investments in **technologies, staff and time**
- Use of technologies for mitigation require commitment to **maintain and monitor**

| Mitigation | VS | Cost |
| --- | --- | --- |
| • Network Monitoring | | • Significant investment in monitoring solution and staff time to monitor |
| • Network Segmentation | | • Additional networking equipment and more advanced skillset to maintain |
| • Backup Testing and Disaster Recover Plans | | • Lower investment in solution and staffing. Reactive response rather than lowering the likelihood or breadth of impact. |

*Balanced investment for risk tolerance and maintainability*

# 03 Cybersecurity Mitigations

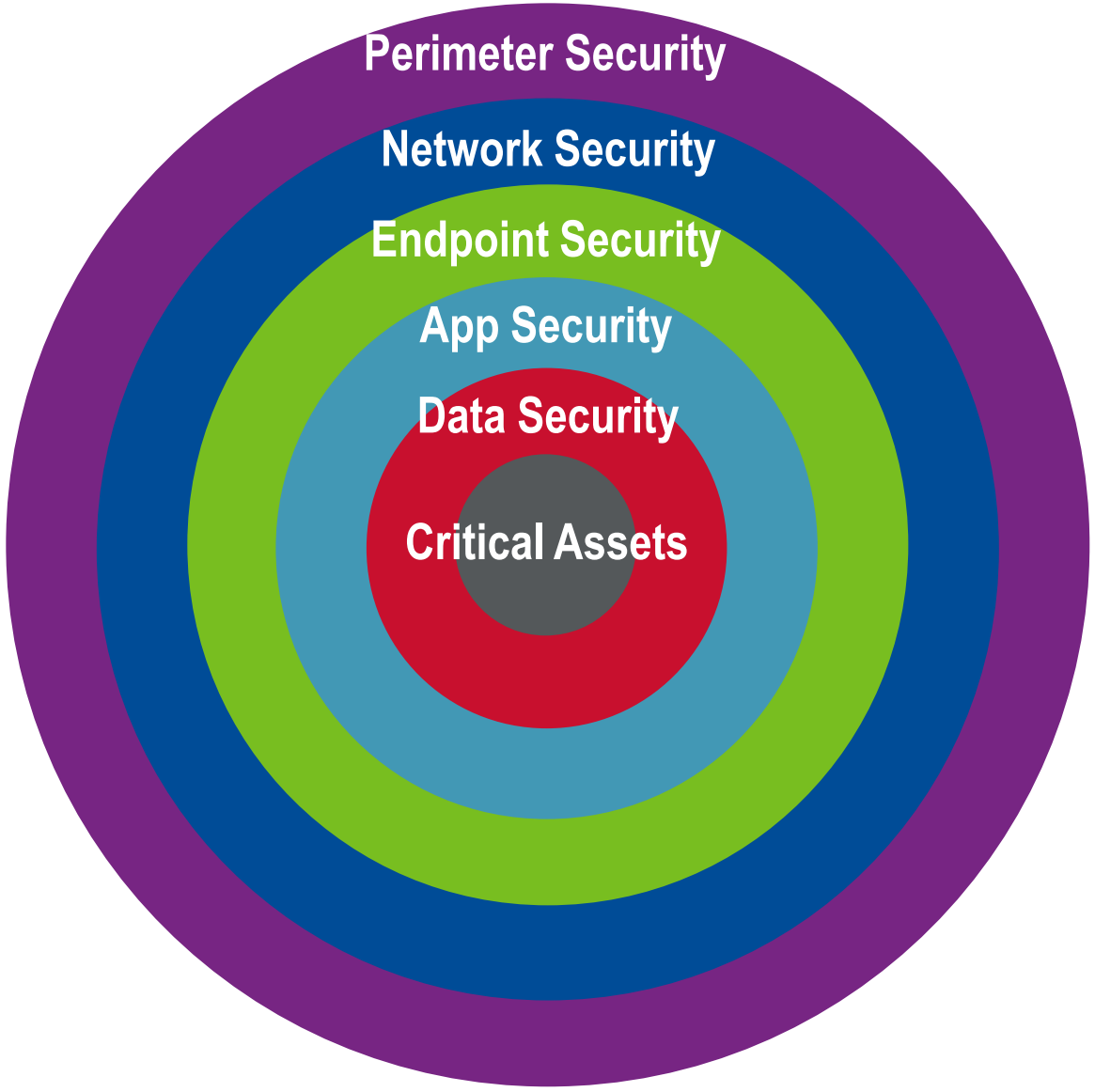
# Context of Remaining Slides

- Focus on **remote access only**
- **High level overview** ~ 15 minutes, too much to cover in detail
- **Best Practices** – per Oldsmar advisories (CISA, WaterISAC, etc.)
- Remote access concepts, **nothing specific to TeamViewer**
- **Management level** presentation - have your technical staff read/follow references at the end
- If slides look familiar . . . HDR presented **“Most Common Cyber Recommendations - Guiding Principles”** at AEA Fall Conference with much of this material . . . please review for a broader perspective

# Defense In Depth

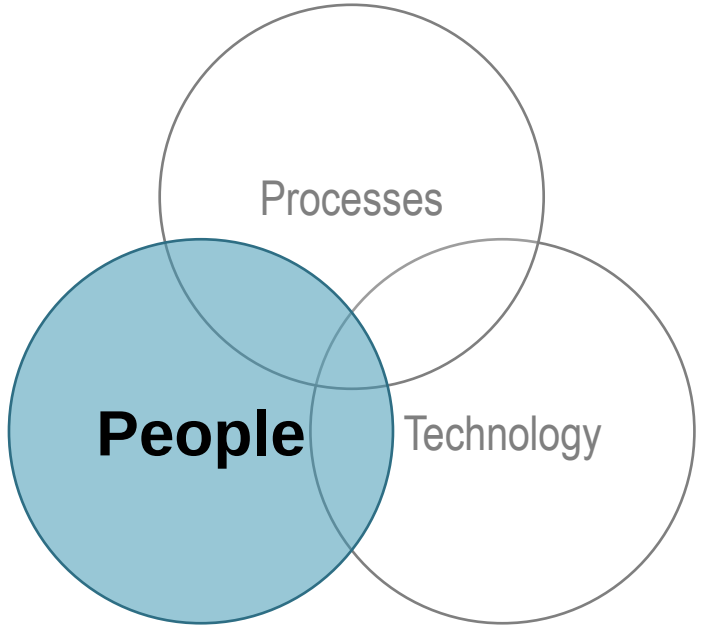
- **Multiple layers** of protection . . . in case one fails
- Includes **abstract concepts**
  - Policies, response, training, etc.
- What are the **crown jewels**?
  - The Historian server?  Or the data?
  - The physical PLC?  Or the programming?
  - The HMI server?  Or the configuration?

*How much would it cost to start over from scratch with OT?*



# PEOPLE, Processes & Technologies

- Establish risk management **leadership** team
- Establish or adopt a risk management **framework**
- Commitment to follow **best practices** and industry **standards**
  - NIST 800-53 (IT Systems)
  - NIST 800-82 (OT Systems)
  - ISA/IEC-62443 (OT Systems)
- **Training** staff on role-specific cybersecurity
- Establish **roles** and **responsibilities**
- **Incident response**, tabletop simulations, and "manual operation" days




*Management support is critical*

# People, PROCESSES & Technologies

- Develop cybersecurity **policies**
  - Set expectations of staff
  - IT and OT systems
  - Include special risk systems - SIS, communications, etc.
  - Many others - see NIST SP800-53
- **Procedures** for system interaction

- **Incident response plans** and **disaster recovery plans** for cyber attacks
- **Risk assessments** at frequency defined by policy
  - Asset Inventory – hardware, software, firmware - you can't protect what you do not know
  - External Connection Inventory – internet, business network, remote sites, etc.
  - Physical (Layer 2) & Logical Drawings (Layer 3)

***Policies & Procedures***

*Get organized and establish a vision for staff*

# People, PROCESSES & Technologies

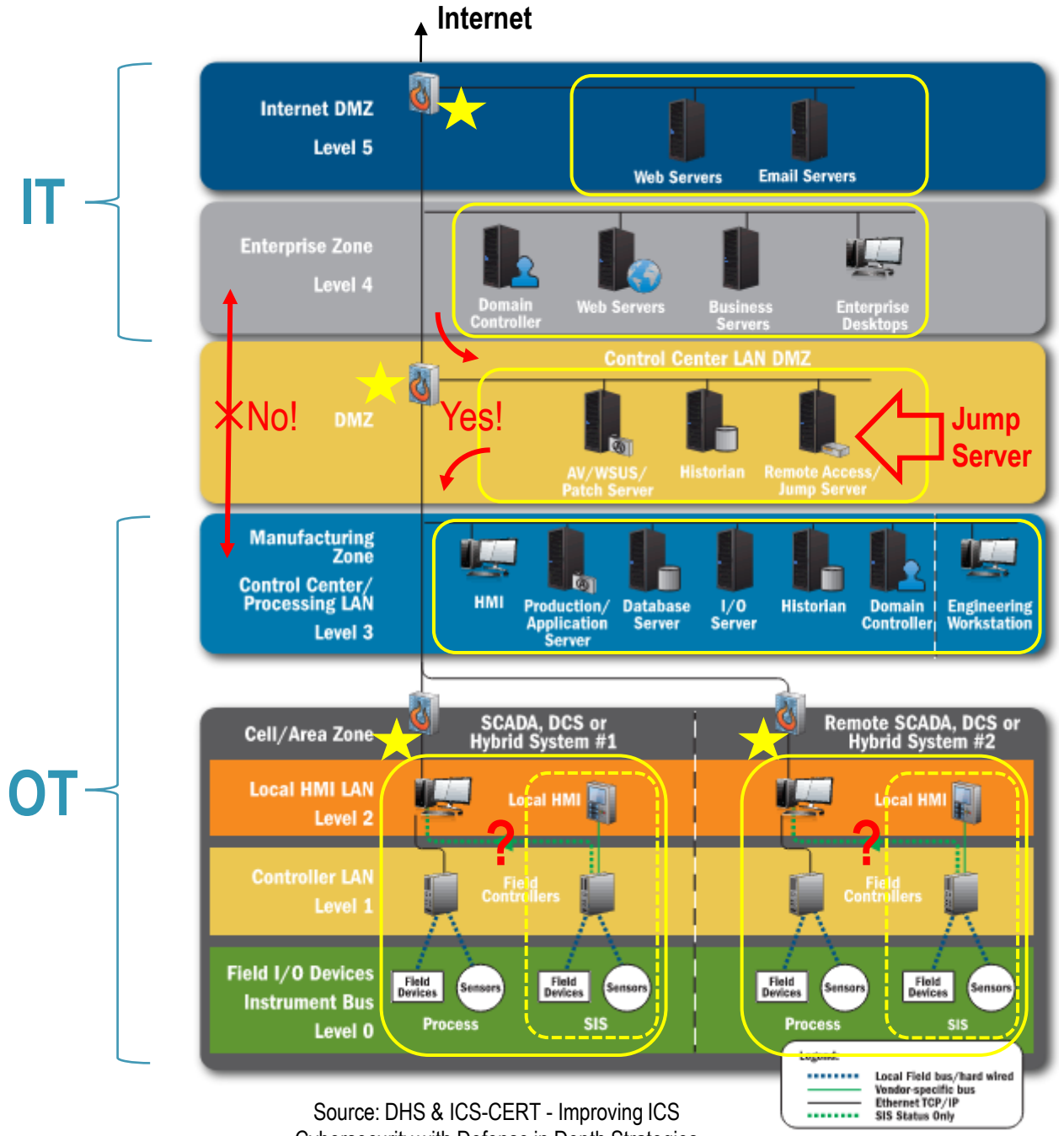
- Password Policy
  - No shared accounts
  - Strong and unique passwords – change often
  - Never store when prompted
- Remote Access Policy
  - Who can access PCS/SCADA?
  - For what purpose and for how long?
  - What security measures are required?
    - Encryption, authentication, authorization, accounting, etc.
  - Who will enable/disable connection?
  - How long before connection times out?
  - Use VPN for encryption, authentication, authorization, and accounting (AAA)
- Access Control Policy
  - Strong multifactor authentication (MFA)
  - Monitor & suspend accounts if suspicious activity
  - Account review – former employees, etc.
  - Authorization creep – multiple job changes
- Audit Policy
  - Confirm endpoint policy compliance
  - Review logs
    - Remote access protocols, suspicious activity
- Subscribe To Notification Services
  - Security alerts, patching

*Policies establish organization expectations*

# People, Processes & TECHNOLOGIES

- **Defense-in-Depth** network architecture
- Like ISA/IEC 62443 **Purdue Model** – Internationally Recognized Standard for connecting IT and OT networks
- **Zones** (networks) & **Conduits** (router/firewall) - segmentation
  - Use conduits to **minimize traffic** between zones!
  - Properly configured firewalls with spam filters, IDS/IPS, VPN, and logging are essential
- Independent **cyber-physical systems**

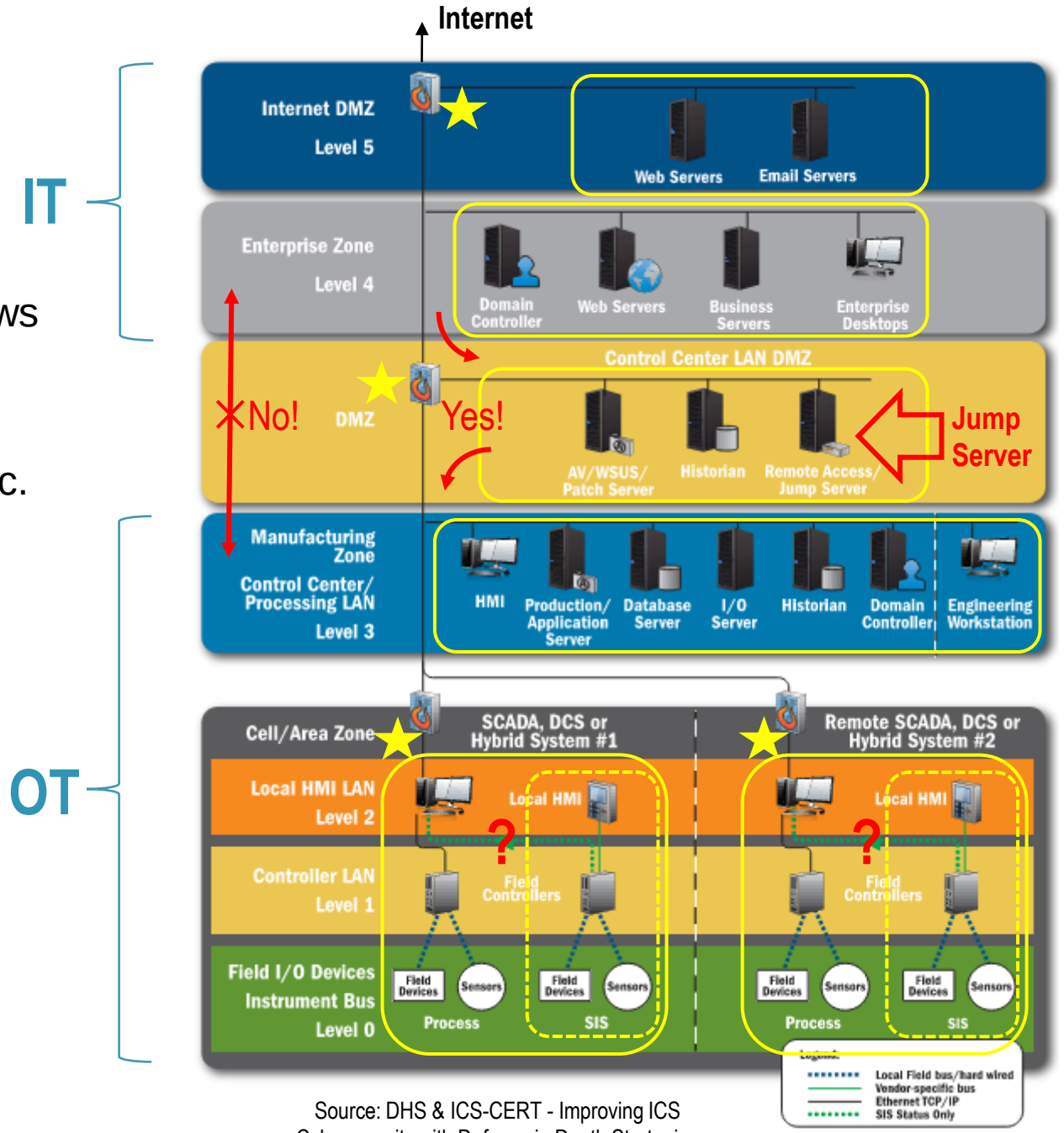
*This may be the #1 recurring theme for OT Cybersecurity*




Source: DHS & ICS-CERT - Improving ICS Cybersecurity with Defense in Depth Strategies

# People, Processes & TECHNOLOGIES

- Segment networks – isolate EoS/EoL
- **Minimize conduit traffic** – only authorized data flows
- Intrusion Detection/Prevention Systems
- Logging – connections, remote access protocols, etc.
- **Encryption** (external data in transit, data at rest)
- **Actively supported operating systems**
- **Patching** (HW, SW, firmware) w/ testbed
- Robust **backup** strategy w/ testbed
- Anti-Malware w/ updates
- Role-based authorization (**least privilege**)
- Endpoint hardening (**least functionality**)




Source: DHS & ICS-CERT - Improving ICS Cybersecurity with Defense in Depth Strategies

# Additional Reading – Oldsmar

See https://www.cisa.gov/tlp for Traffic Light Protocol (TLP)

- 2021-03-02 **JRIC** - TLP:GREEN Compromise of US Water Treatment Facility Highlights Vulnerability of Critical Infrastructure to Cyber Attacks (pdf) – **1 page**
- 2021-02-16 **WaterISAC** - Even the Basics are Critical for Critical Infrastructure (web) – **4 pages**
- 2021-02-11 **CISA** - TLP:WHITE AA21-042A Joint Cybersecurity Advisory Compromise of U.S. Drinking Treatment Facility (pdf) – **4 pages**
- 2021-02-09 **WaterISAC** - (U//FOUO) Joint Situational Report on Recent Water Sector Cybersecurity Incident (web) – **4 pages**
- 2021-02-08 **WaterISAC** - Malicious Actor Compromises U.S. Water Treatment Plant, Changes Chemical Level (web) – **3 pages**

*Ensure tech staff read and follow these guidance documents*

# Additional Reading – Basics

- 2020-07-23 **CISA** - NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems (pdf) – **5 pages**
- 2019-09-04 **AWWA** - Water Sector Cybersecurity Risk Management Guidance (pdf) – **58 pages**
- 2019-06-04 **WaterISAC** - 15 Cybersecurity Fundamentals for W/WW Utilities (pdf) – **56 pages**
- 2017-08-21 **EPA** - Incident Action Checklist – with 2021-02 update (pdf) – **6 pages**
- 2016-11-14 **EPA** - Cybersecurity Guide For States (pdf) – **4 pages**
- 2016-09-22 **DHS & ICS-CERT** - Improving ICS Cybersecurity with Defense-in-Depth Strategies (2016) – **58 pages**

*Ensure tech staff read and follow these guidance documents*

**You have to be right 100% of the time, the cyber criminals only have to be right once!**

04

# Q&A / FAQs

# Questions?

**David Brearley, GICSP, PMP**
Operational Technology Cybersecurity Director
David.Brearley@hdrinc.com | (704) 338-6853

**Jim Schultz, P.E., CISSP, GICSP, CCNA, C|EH**
Cybersecurity Network Engineer
James.Schultz@hdrinc.com | (215) 845-6714

## Additional Information:

- Water ISAC
- AWWA Cybersecurity Guidance
- CISA
- ICS-CERT
- ISA-62443
- NIST 800-82
- NIST 800-53