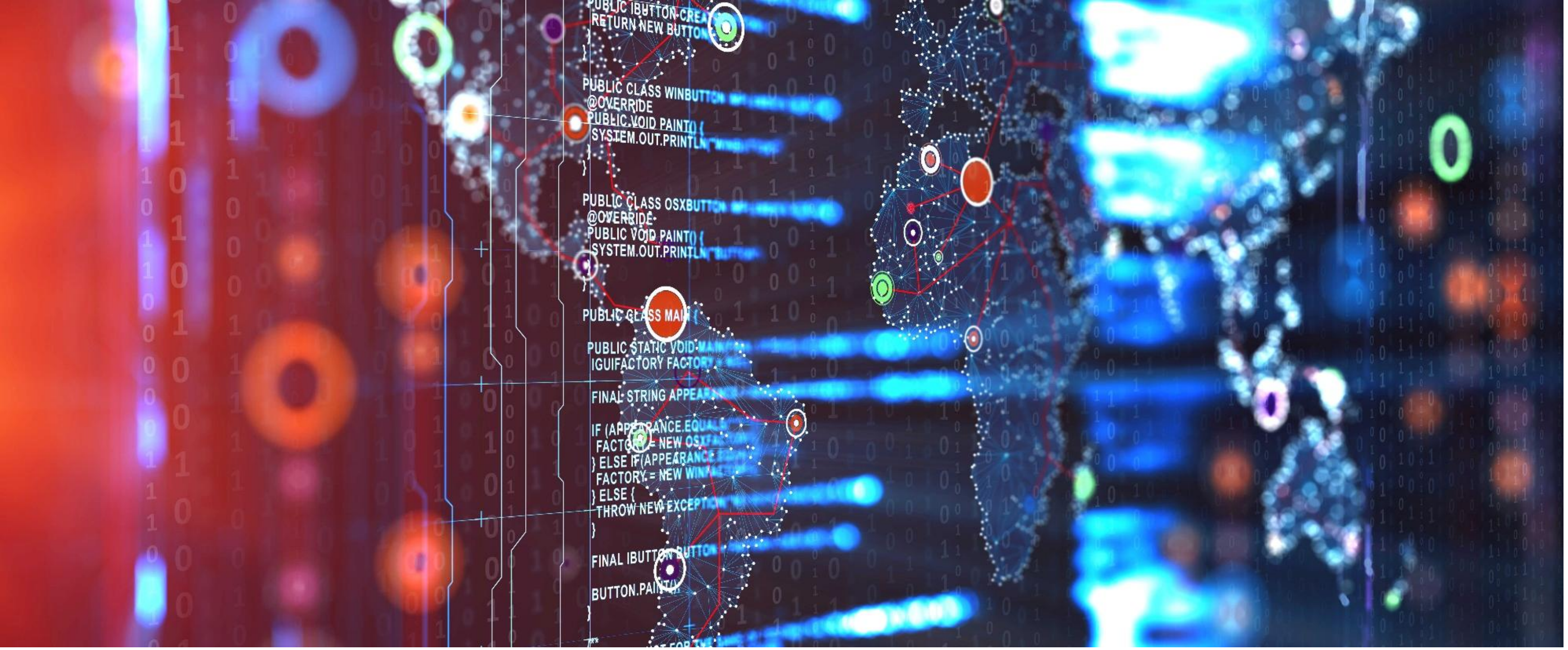


Developing Cyber Risk Awareness and Mitigation: Be Prepared!

HDR

11/13/2020

Presenters

David Brearley, GICSP, PMP

Program Manager, Cybersecurity

David.Brearley@hdrinc.com

Jim Schultz, P.E., CISSP, GICSP, CCNA

Cybersecurity Engineer

James.Schultz@hdrinc.com

AGENDA

01 Operational Technology Threat Landscape

02 Cybersecurity Guiding Principles

03 Additional Resources

04 Q&A / FAQs

01

Operational Technology Threat Landscape

Remote Access

IIoT/IoT

Recovery after disaster or catastrophic failure

Data Analytics

situational awareness

Network security

A leaner, mobile work force

Preparation for a major expansion

Need to utilize data to drive business decisions

Dependence on proprietary system

Behind advances in technology

Cloud Computing

Improve system communications

Need for process control optimization

Nuisance alarms

Poor system performance

Security

Optimization

Reliability

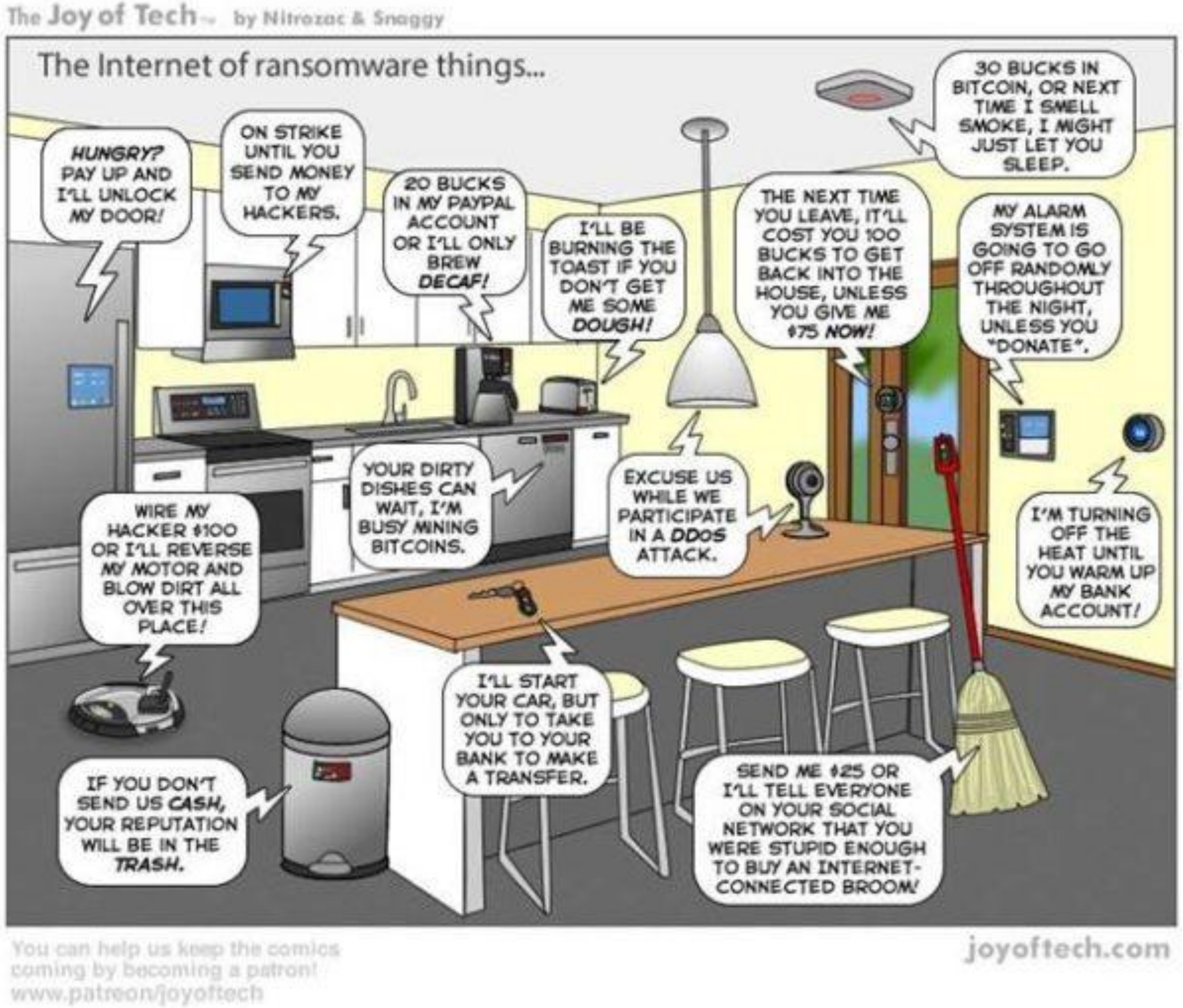
Resiliency

The Connected Enterprise

- Cybersecurity = Risk Management

Convenience	vs.	Risk
Remote Access		OT exposure to business networks/internet
Mobility		Potential for Wireless and personal device exposure
SCADA & Business Integrated Data (LIMS/CMMS/WMMS)		OT exposure to business networks and personnel
IT staff management of OT (ICS)		IT staff not familiar with plant requirements

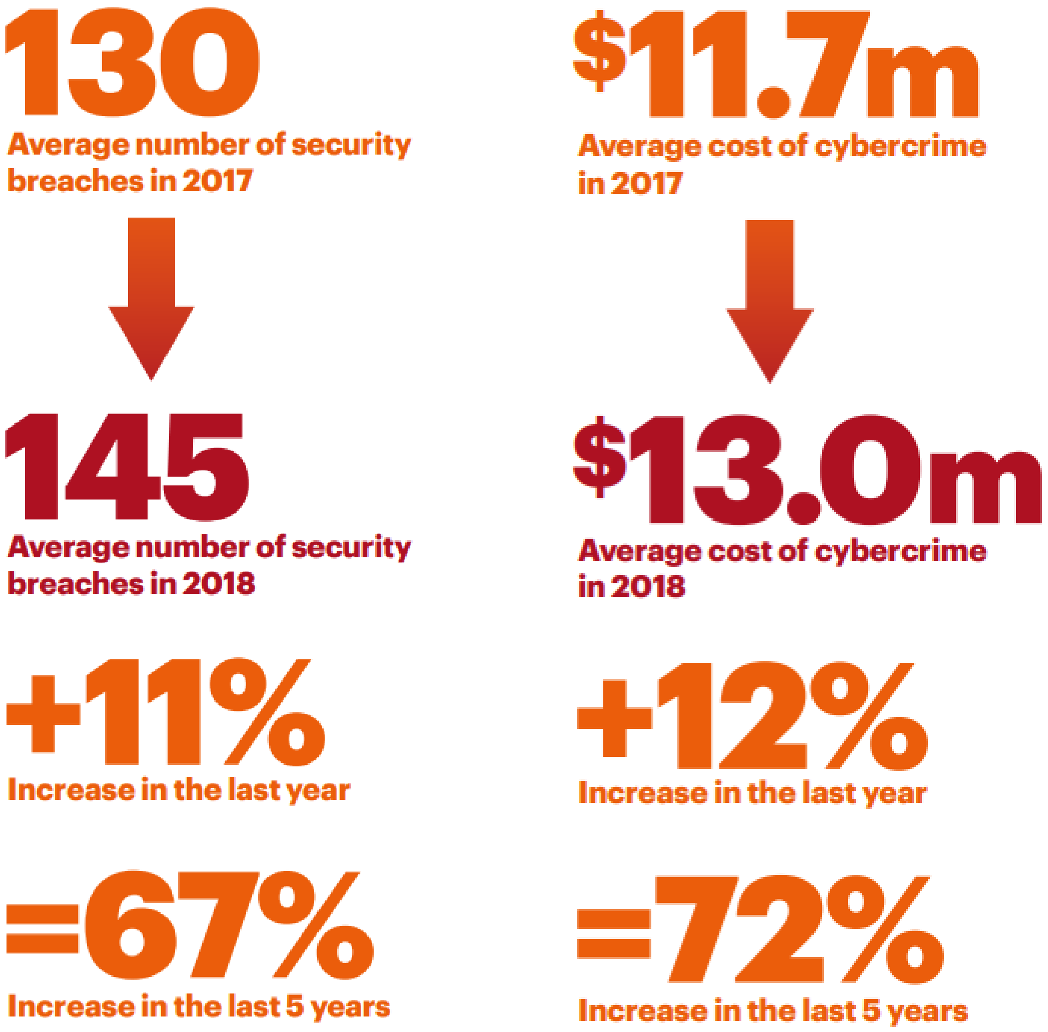
- Increase in networked devices = larger attack surface
- Additional Maintenance / Patching


The Joy of Tech by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

So What?

City Risk Matrix

- Reputation
- Safety
- Regulatory
- Environmental
- Legal
- Financial



130
Average number of security breaches in 2017

145
Average number of security breaches in 2018

+11%
Increase in the last year

=67%
Increase in the last 5 years

$11.7m
Average cost of cybercrime in 2017

$13.0m
Average cost of cybercrime in 2018

+12%
Increase in the last year

=72%
Increase in the last 5 years

Source: Accenture 2019 Cost of Cybersecurity Crime Report

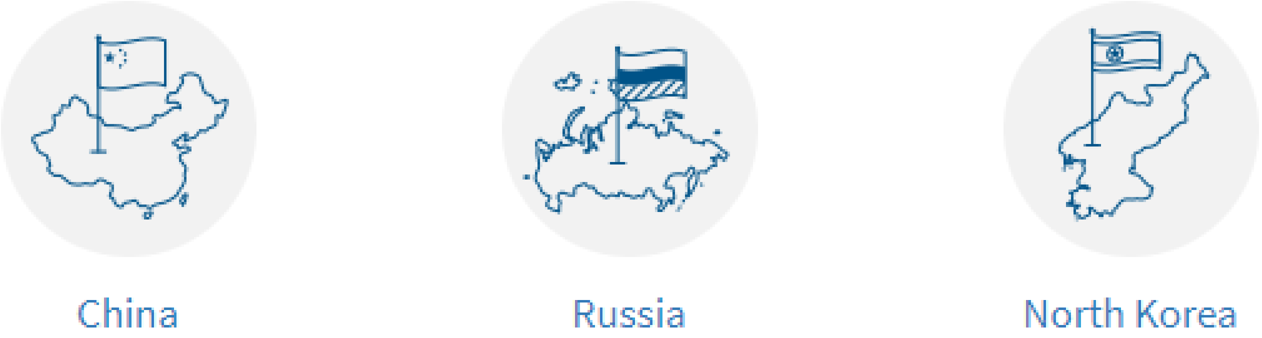
Elimination of all risk is not possible or affordable

Who is the adversary?

General Classifications

- Insider Threat / Outsider Threat
  - Motivated vs. Non-Motivated
  - Skilled vs. Unskilled

Cybersecurity & Infrastructure Security Agency (CISA)
Current Nation States Threats



Outside Groups

- Nation States
- Ransomware as a Service (RaaS)
- Hacking Groups
- Activists, disgruntled individuals
- Many other possibilities…. Students, grandma’s computer, any connected device. 14-year-old kid

Successful Attacks

- 2020 (July): Israel Water System (Agriculture Pump Stations)
- 2020 (April): Israel Wastewater Treatment Plants & Pump Stations
- 2020: Greenville, SC Water System – Online Payment and Phones
- 2019: Triconex Safety System Attacks (multiple)
- 2019: Simultaneous attack on 22 Texas Cities
- 2018: Onslow Co, NC Malware Attack
- 2018: Atlanta, GA / Baltimore, MD Ransomware (~$17M each)
- 2017: US Water System (undisclosed) cellular attack
- 2016: Kemuri Water Co (KWC) Chemical Dosing Changes
- 2016: Ukraine power grid
- 2014: Smart Meter Attacks (5 Cities)
- 2013: Bowman Ave Dam, NY
- 2012: IL Municipal Water (From Russia w/Love)
- 2010: STUXNET
- 2009: Texas road sign Zombies
- 2000: Marooshy Shire, Au Sewage Spill

*"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

Self-Induced Cyber Attacks

SE Linear Accelerator

2013: an update by personnel resulted in a reboot, causing the patient to receive a double dose of radiation

SCADA

2011: an update by support staff resulted in the SCADA system failing. This system serves all the utilities in Metro San Diego

Catheter Lab

2014: an update by personnel resulted in a reboot, nearly causing death of the patient

Myths & Misconceptions

- We don’t need patching/updates
- Too small to be hacked
- Our Systems Integrator…
- Our IT Staff…
- We know our staff would never…

02 Cybersecurity Guiding Principles

America's Water Infrastructure Act 2018

- Risk & Resilience Assessment
  - Includes cybersecurity
  - 20+ projects completed – focused on operational technology (OT)
  - Large, medium, small utilities (by customers served)
  - **What are the most common recommendations?**
  - We call them Guiding Principles . . . a good start down the road to cybersecurity
  - The goal of this presentation is to inspire others to go out and learn more about these topics

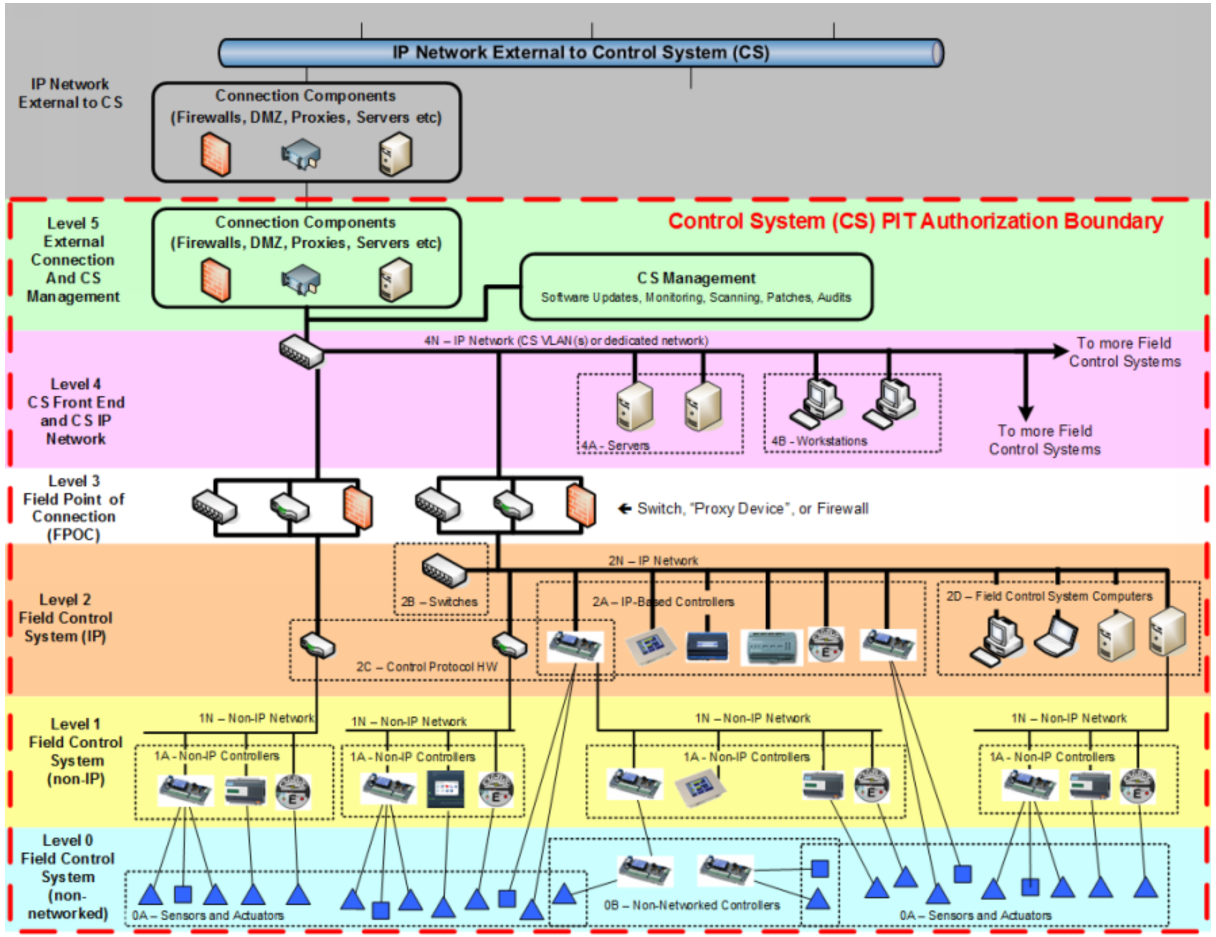
Cybersecurity Guiding Principles

- PCS/SCADA System Documentation
- Ransomware Protection
- ISA/IEC 62443 Architecture
- Defense In Depth
- Physically Separate IT/OT Networks
- Network Segmentation
- Secure Remote Access
- Perimeter Protection
- Removable Media
- Mobile Devices
- Wi-Fi Access
- Physical Protection
- WaterISAC 15
- AWWA Cybersecurity Guidance

Cybersecurity Guiding Principles

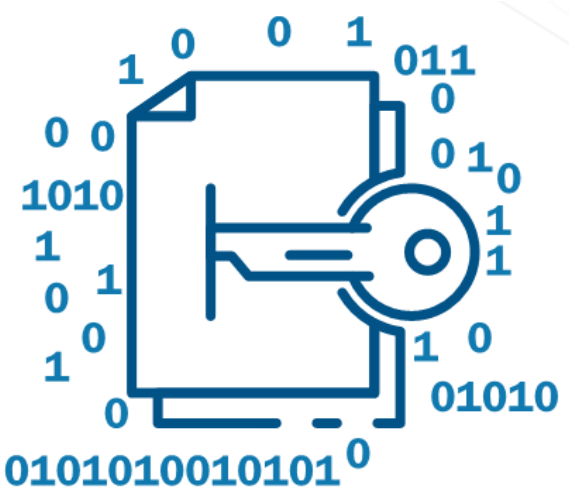
- PCS/SCADA System Documentation
  - Asset inventory
    - Use this to track if OS/application updates available?
  - Physical network drawings (OSI Layer 2)
  - Logical network drawings (OSI Layer 3)
  - Policies & procedures
    - The human is the weakest link and policies can really help

You can't defend what you don't know about.


IP Network External to Control System (CS)
IP Network External to CS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Control System (CS) PIT Authorization Boundary
Level 5 External Connection And CS Management
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
CS Management
Software Updates, Monitoring, Scanning, Patches, Audits
4N – IP Network (CS VLAN(s) or dedicated network)
To more Field Control Systems
Level 4 CS Front End and CS IP Network
4A - Servers
4B - Workstations
To more Field Control Systems
Level 3 Field Point of Connection (FPOC)
← Switch, "Proxy Device", or Firewall
2N – IP Network
Level 2 Field Control System (IP)
2B – Switches
2A – IP-Based Controllers
2D – Field Control System Computers
2C – Control Protocol HW
Level 1 Field Control System (non-IP)
1N – Non-IP Network
1N – Non-IP Network
1N – Non-IP Network
1N – Non-IP Network
1A - Non-IP Controllers
1A - Non-IP Controllers
1A - Non-IP Controllers
1A - Non-IP Controllers
Level 0 Field Control System (non-networked)
0A – Sensors and Actuators
0B – Non-Networked Controllers
0A – Sensors and Actuators

Source: DoD UFC 4-010-06 Cybersecurity for FRCS

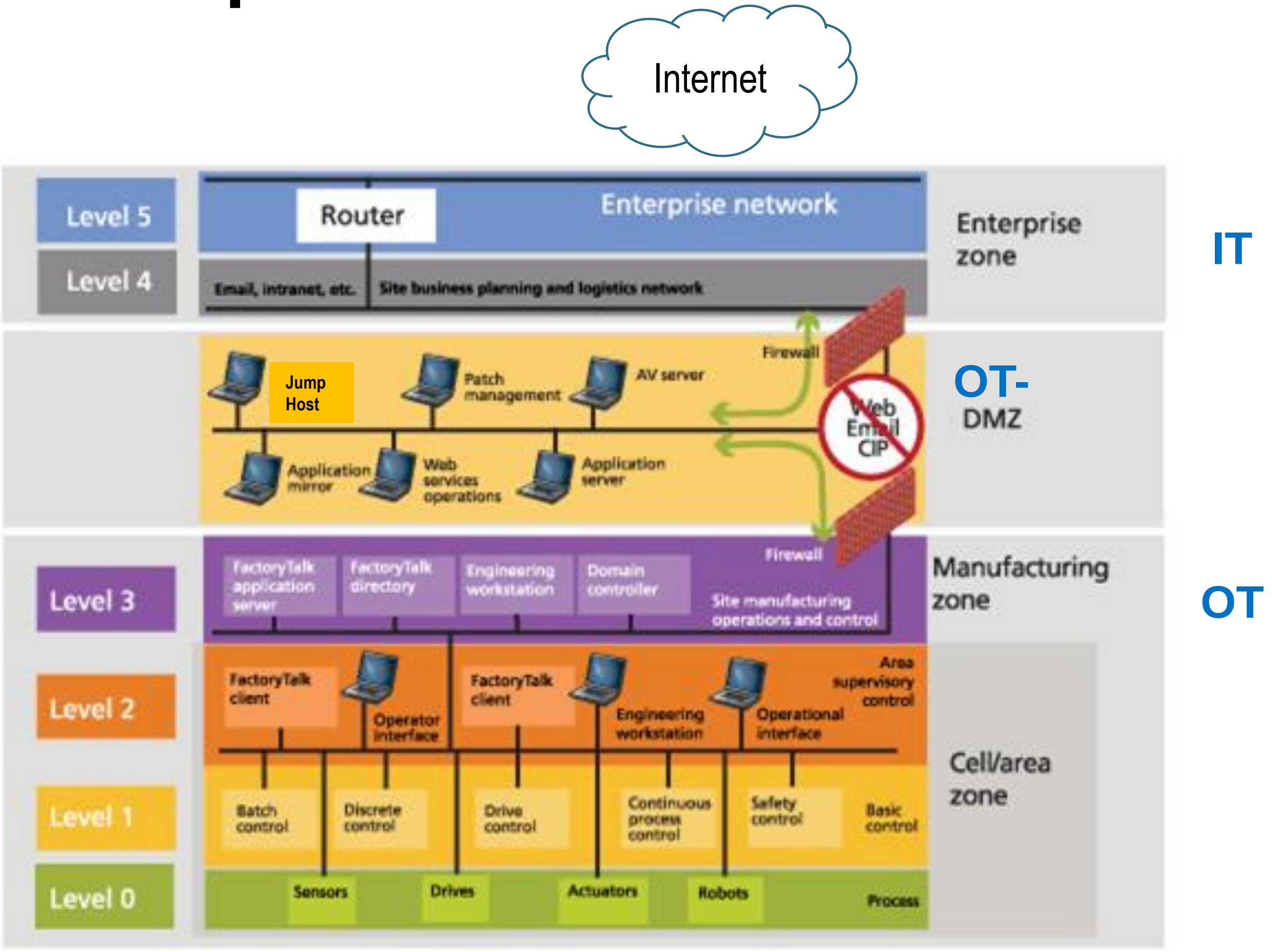
Cybersecurity Guiding Principles



- Ransomware Protection
  - Keep up with patching/updates – use a testbed
    - OS, applications, firmware
    - Verify authenticity
  - Disaster recovery – online, offline, offsite backups
    - OT backups w/ periodic validation testing
    - APT can go undetected for 6+ months
    - Keep one year or more of backups
  - Emergency Response Plan (ERP)
    - Add OT content to at least restore local manual control (e.g. OIT, PLC, I/O, etc.)
  - Harden endpoints – least functionality, least privilege
  - Additional reading: CISA MS-ISAC Ransomware Guide S508C.pdf

Cybersecurity Guiding Principles

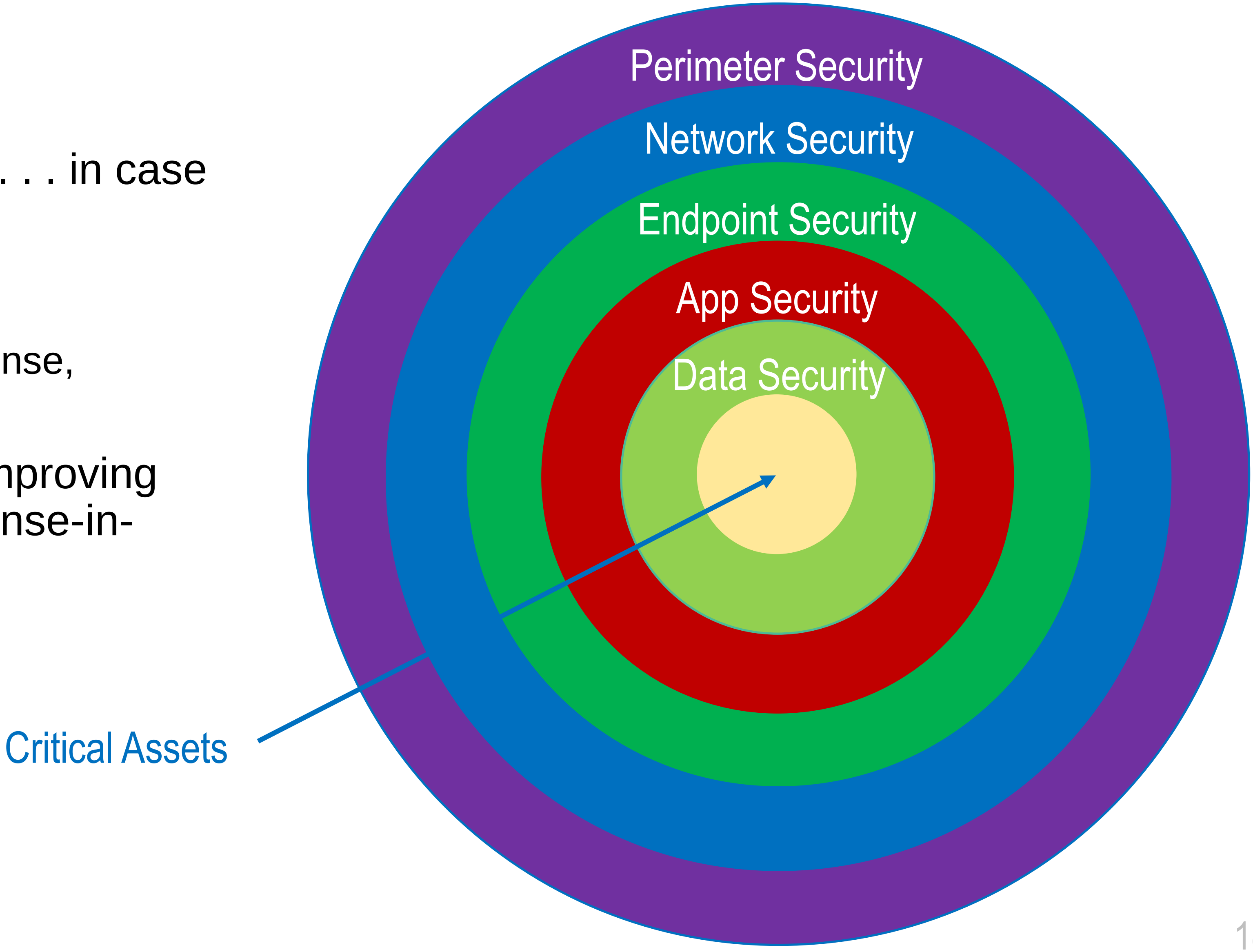
- ISA/IEC 62443 Architecture
  - Internationally recognized standard
  - Purdue Model
  - No direct communication between IT and OT networks
  - IT and OT networks can initiate comms, but not OT-DMZ
  - Not a silver bullet – trying to increase work effort of adversary to allow detection
  - Additional reading: www.isa.org



Source: https://www.isa.org/intech/20140806/

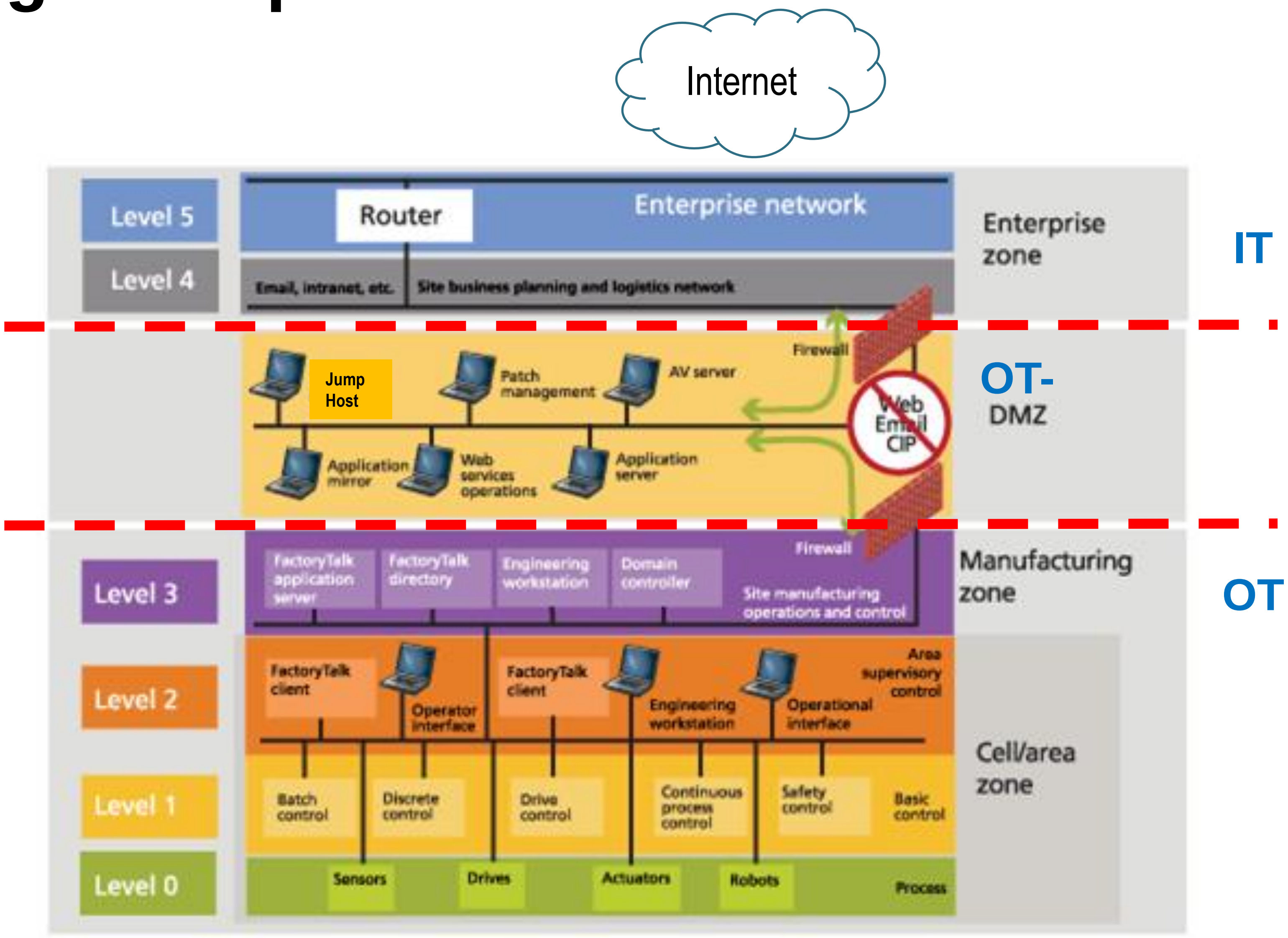
Cybersecurity Guiding Principles

- Defense In Depth
  - Multiple layers of protection . . . in case one fails
  - Includes abstract concepts
    - Policies, monitoring, response, training, etc.
  - Additional reading: CISA - Improving ICS Cybersecurity with Defense-in-Depth Strategies



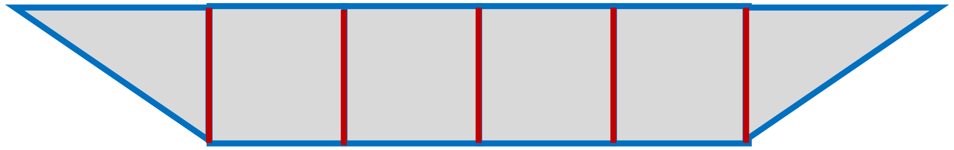
Cybersecurity Guiding Principles

- Physically Separate IT/OT Networks
  - Separate switches, not VLANs
    - IT: Internet, Email, VoIP, Cameras, Access Control
    - OT: PCS, SCADA
  - Separate VM Hosts
  - No "multi-homing“ – except PLCs
  - Additional reading: NIST SP800-82r2



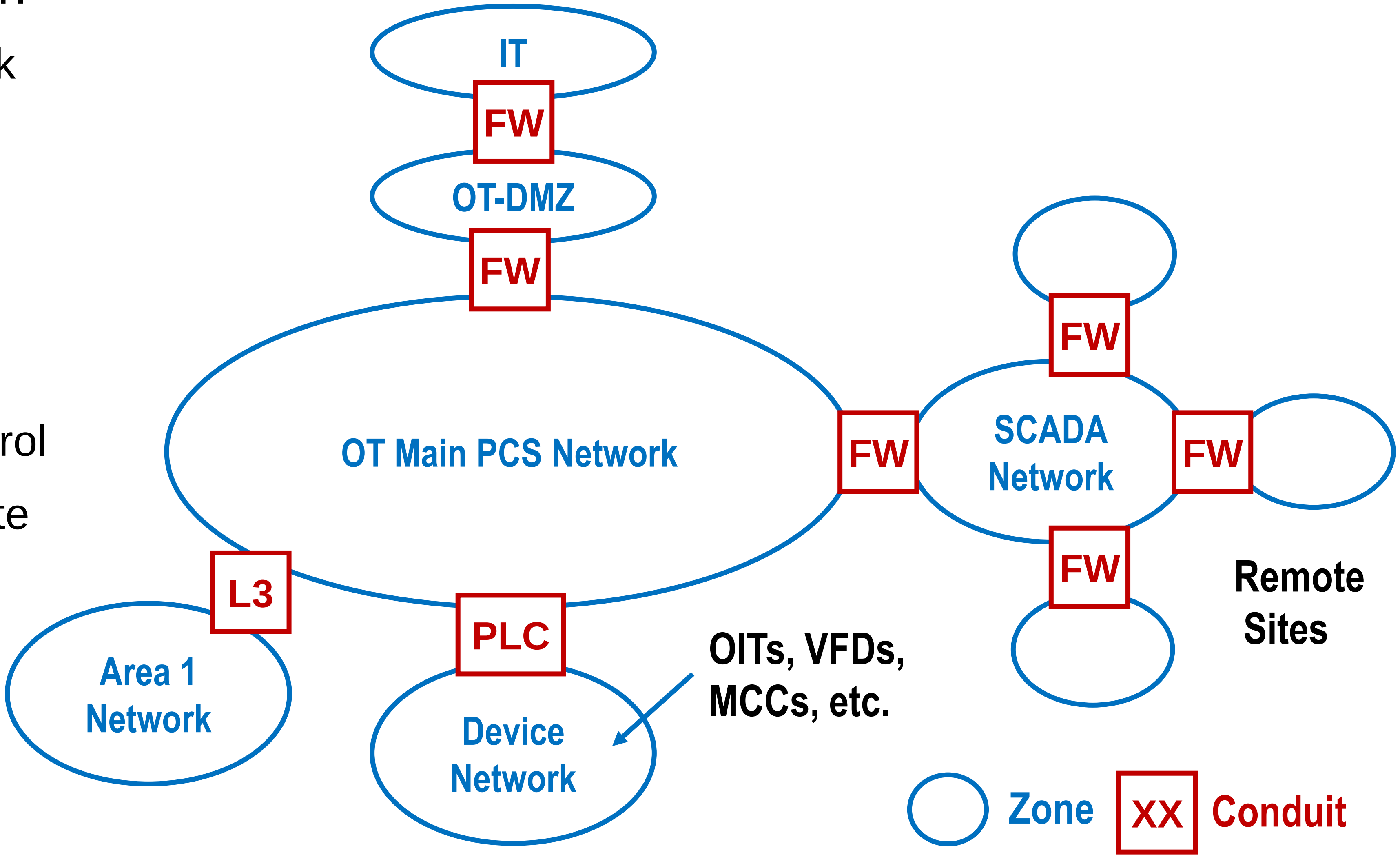
Source: https://www.isa.org/intech/20140806/

Cybersecurity Guiding Principles



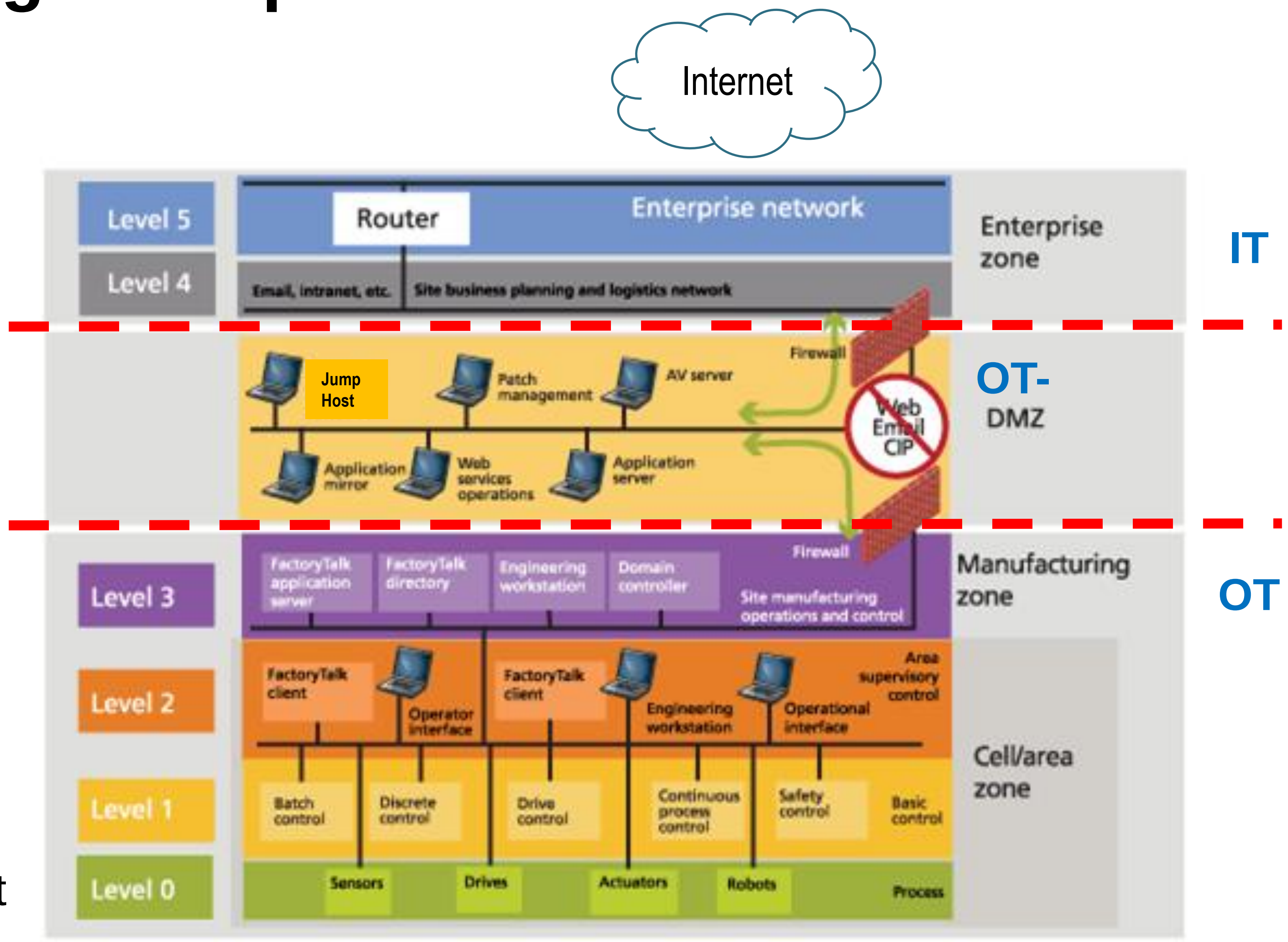
e.g. Ship Bulkhead

- Network Segmentation
  - Not just one big network
  - "Zones & Conduits" per ISA/IEC 62443
    - Zones are networks
    - Conduits filter traffic
  - Can help limit damage and preserve local control
  - Encryption of remote site communications is essential
  - Additional reading: NIST SP800-82r2



Cybersecurity Guiding Principles

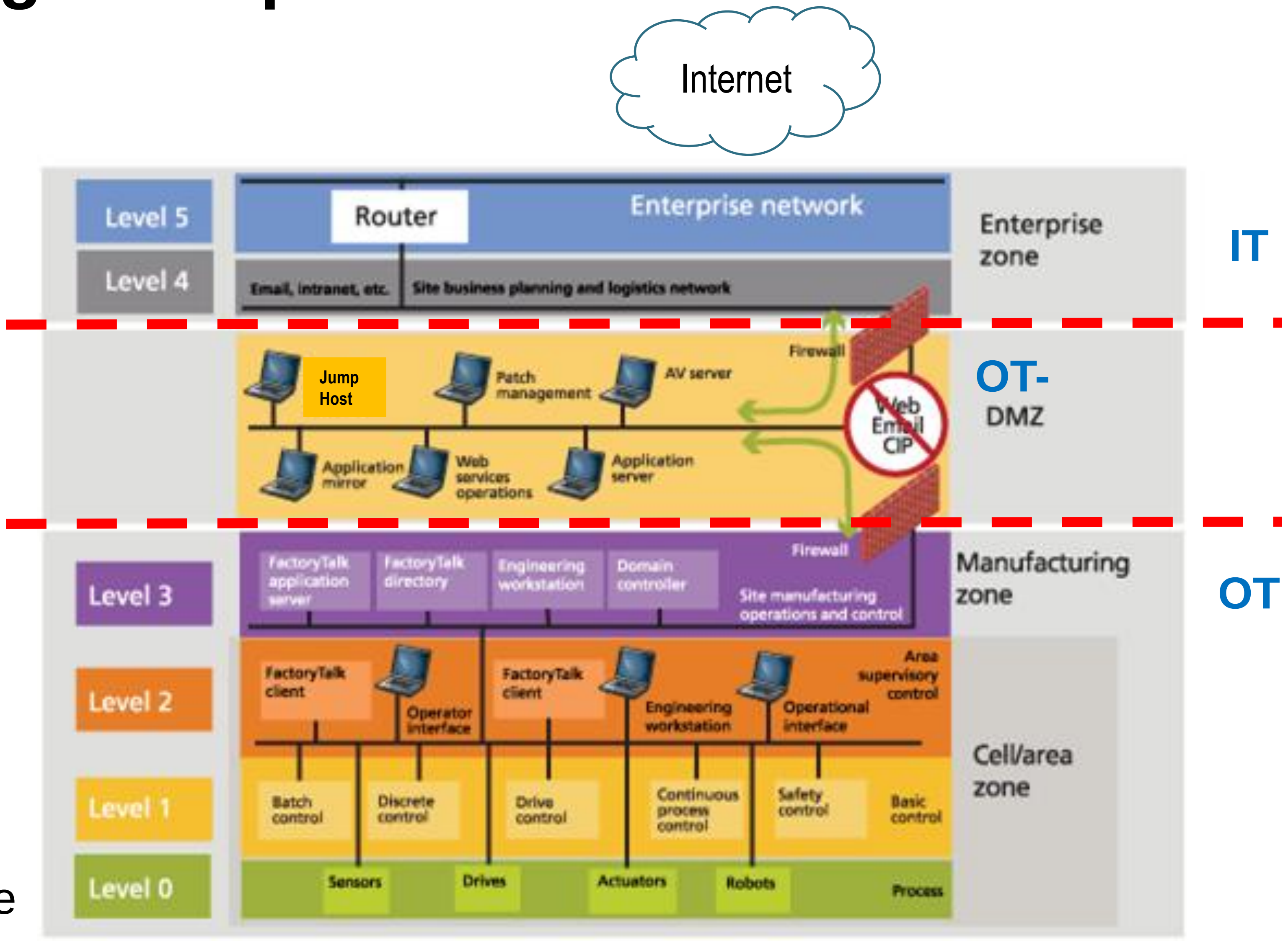
- Secure Remote Access
  - Policies and procedures
  - For maintenance only
  - Dedicated utility laptops, <u>minimal</u> capability
  - "Jump Host", no direct access
  - Virtual Private Networks for encryption & authentication
    - Only as secure as connected devices, not silver bullet
  - Multi-factor authentication
  - Remote Desktop – popular, but vulnerable (e.g. ransomware)



Source: https://www.isa.org/intech/20140806/

Cybersecurity Guiding Principles

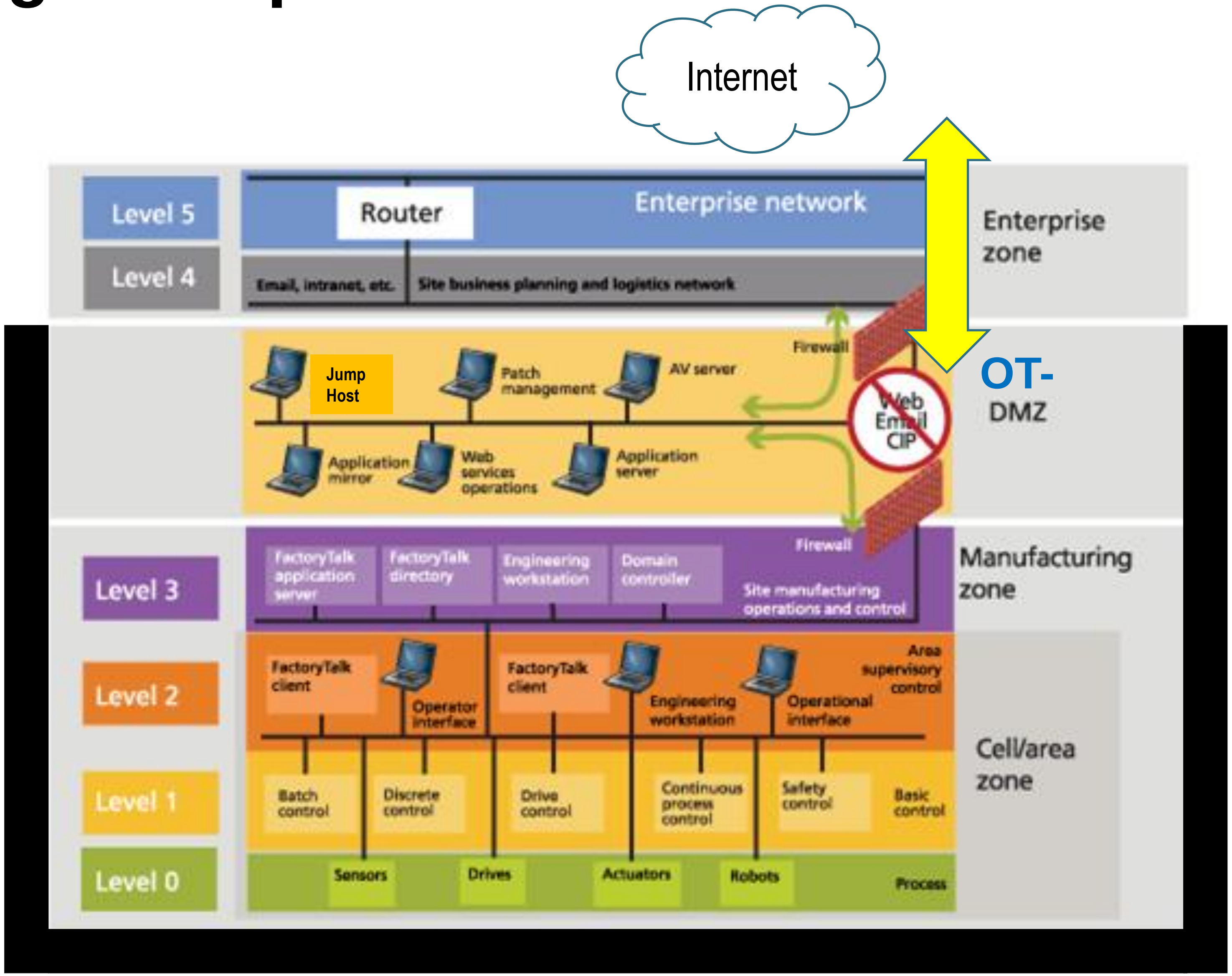
- Secure Remote Access
  - Operator supervision/control
  - Enforce time limits
  - Maximize logging
  - Network access control
  - Intrusion detection
  - Least functionality throughout
  - Least privilege throughout
  - Additional reading: WaterISAC 15, CISA - Improving ICS Cybersecurity with Defense-in-Depth Strategies, and lots more



Source: https://www.isa.org/intech/20140806/

Cybersecurity Guiding Principles

- Perimeter Protection
  - No "backdoor" connections to PCS/SCADA
  - No cell modems, analog modems, phone lines, IoT gateways, etc.
- Remote site polling, at least, through a firewall
- One-Way In & One Way Out: The OT-DMZ
  - Support via "Jump Host"
  - WIN-911 Notifications via "Email Relay" in OT-DMZ

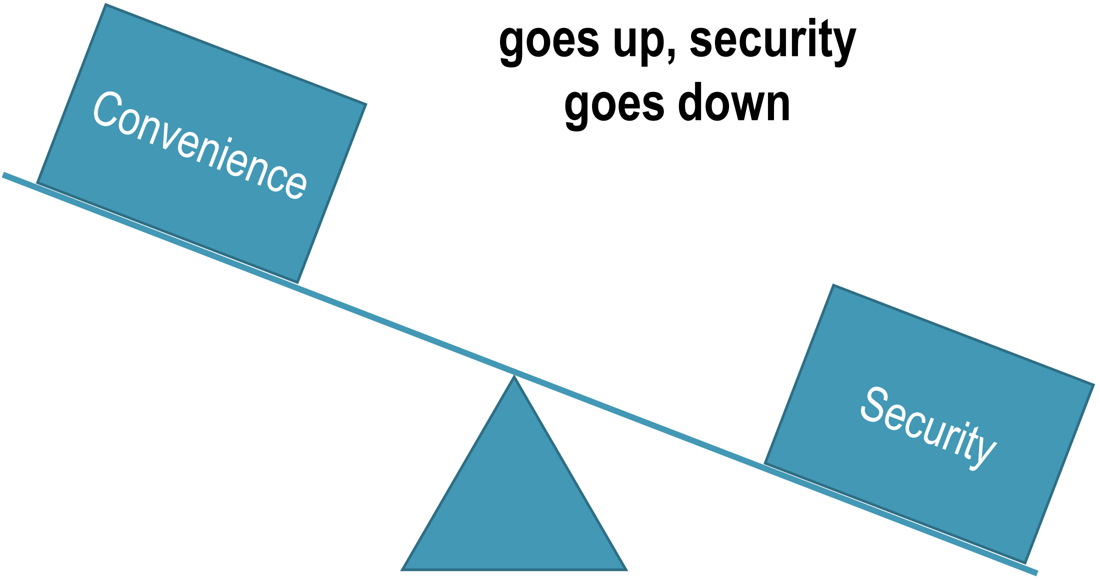


Cybersecurity Guiding Principles

- Removable Media Management
  - But we're air-gapped . . .
  - APT malware designed to jump air gaps
    - Ramsay, Turla, MiniDuke, RedOctober, Fanny, Remsec, Stuxnet
  - Policy, procedures, training, patching/updates, enforcement
  - AV kiosk, no personal media
  - Concept applies to laptops too!
  - Additional reading: Control Engineering - "Eight steps for managing removable media use in critical infrastructure environments"

Cybersecurity Guiding Principles

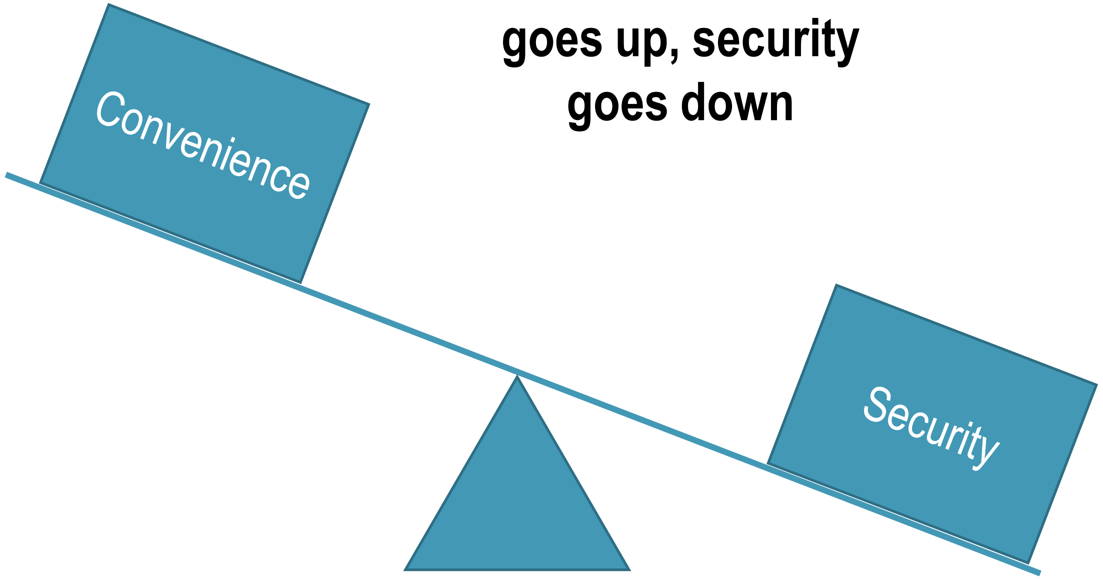
- Mobile Devices
  - Risk-based decision
  - Understand your risk and risk tolerance
  - Increases convenience, reduces protection
    - Bigger attack surface
    - Free apps: You are the product
    - Apple/Android have significant control over security
    - Not recommended for PCS/SCADA
  - Mobile Device Management (MDM) can help
  - Policy, procedures, training, enforcement, patching/updates can help
  - Accessing an HMI web portal and not PCS/SCADA directly can help
  - No known good references for securely using mobile devices with PCS/SCADA



When convenience goes up, security goes down

Cybersecurity Guiding Principles

- Wi-Fi Access
  - Risk-based decision
  - Understand your risk and risk tolerance
  - Increases convenience, reduces protection
    - Bigger attack surface
    - Lots of free software to hack Wi-Fi
    - Not recommended for PCS/SCADA
    - WPA2 is the best available Wi-Fi option but is still vulnerable
  - A WPA2 Wi-Fi solution based on 802.1X EAP-TLS authentication can help
  - A Wireless Intrusion Detection System (WIDS) can help
  - Policy, procedures, training, enforcement, patching/updates can help
  - No known good references for securely using Wi-Fi devices with PCS/SCADA



When convenience goes up, security goes down

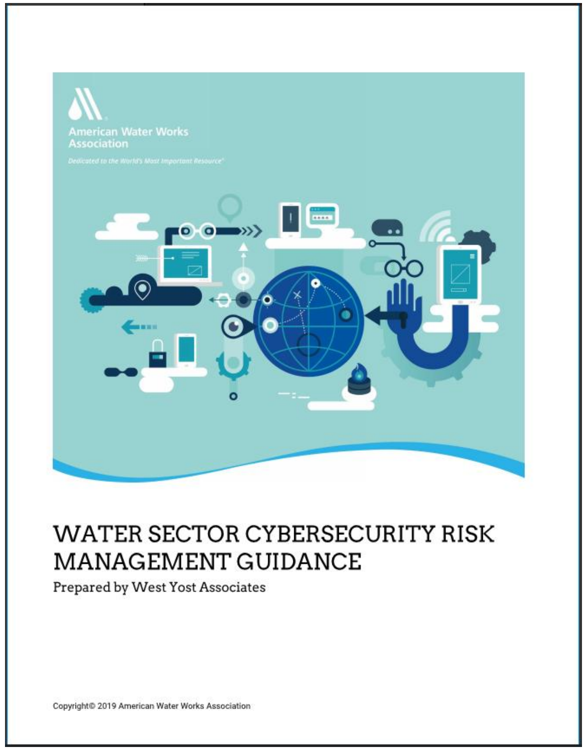
Cybersecurity Guiding Principles

- Physical Protection
  - Locks
  - Cameras
  - Physical intrusion detection systems
  - Physical access control systems
  - Additional reading: NIST SP800-53r4

You can't have cybersecurity without physical security.

Cybersecurity Guiding Principles

- Don't forget these great resources
  - WaterISAC 15
  - AWWA Cybersecurity Guidance & Tool
    - Reworked to support AWIA 2018 compliance



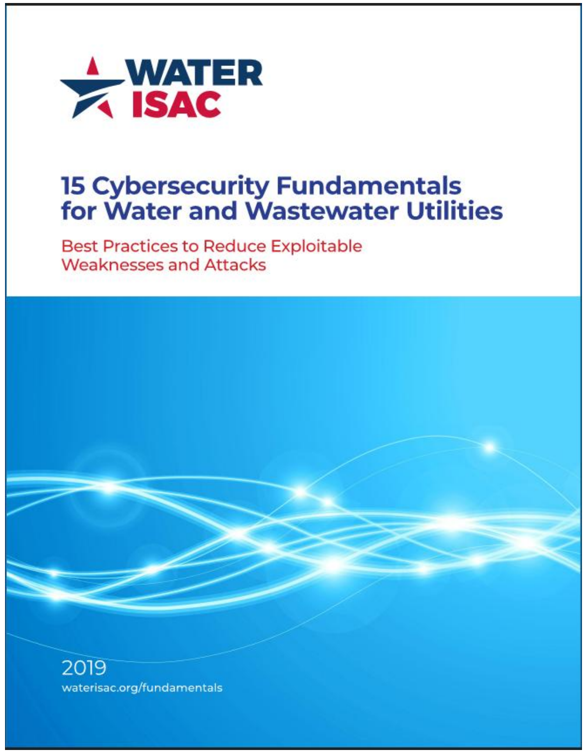
American Water Works Association

Dedicated to the World's Most Important Resource®

WATER SECTOR CYBERSECURITY RISK MANAGEMENT GUIDANCE

Prepared by West Yost Associates

Copyright© 2019 American Water Works Association



WATER ISAC

15 Cybersecurity Fundamentals for Water and Wastewater Utilities

Best Practices to Reduce Exploitable Weaknesses and Attacks

2019

waterisac.org/fundamentals

03 Additional Resources

Executive Order 13636 and PPD-21

- Executive Order 13636: Improving Critical Infrastructure Cybersecurity directs the Executive Branch to:
  - Develop a technology-neutral voluntary cybersecurity framework
  - Promote and incentivize the adoption of cybersecurity practices
  - Increase the volume, timeliness and quality of cyber threat information sharing
  - Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
  - Explore the use of existing regulation to promote cyber security
- Presidential Policy Directive-21: Critical Infrastructure Security and Resilience replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:
  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - Understand the cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - Develop comprehensive research and development plan

Cybersecurity Legislation

- https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx
- Pending or Enacted Categories
  - Cyber Incident Reporting
  - Freedom of Information Act Protections for Cybersecurity Info
  - Inclusion of Cybersecurity in Disaster Definitions
  - Planning Committees and Other Assessments
  - Insurance Requirements
  - Prosecution for Cyber Crime
  - Training
- America’s Water Infrastructure Act (October 2018)

Cybersecurity Standards and Guidelines

Guidelines

- AWWA Cybersecurity Guidance Portal
  - Self-Assessment Tool
- Cybersecurity and Infrastructure Security Agency (CISA)
- DHS ICS-CERT
- NIST Cybersecurity Framework (CSF)

Standards

- ISA-62443
- NIST SP800-53
- NIST SP800-82

Threat Intelligence Sources

- InfraGard
- Water ISAC
- ICS-CERT Advisories

04

Q&A / FAQs

Q&A / FAQs

Question: Who would ever hack a water / wastewater plant?

- Response: Anyone looking to cause harm to the utility or public is a potential adversary.

Question: My system is “air gapped”, doesn’t this make me safe?

- Response: No, air gapped systems are . . . vulnerable to insider attack, rely on humans to control/restrict introduction of risk, have a tendency to be unmonitored and not patched

Question: I’m new to cyber, what are some good resources to increase my knowledge?

- Response: ICS-CERT Free Training (https://us-cert.cisa.gov/ics/Training-Available-Through-ICS-CERT)

Question: How to I fund cybersecurity?

- Response:
  - Integrate control systems into asset management planning
  - Early engagement of cybersecurity in projects reduces costs and impact to operations
  - Develop ROI metrics to justify cost of mitigations vs. potential impacts of an event

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