Jacobs Challenging today. Reinventing tomorrow.

Awareness & Vigilance Help Prevent Cyber-Tampering at Water Treatment Facilities

In the kNOW Webinar Series

March 3, 2021

Speakers

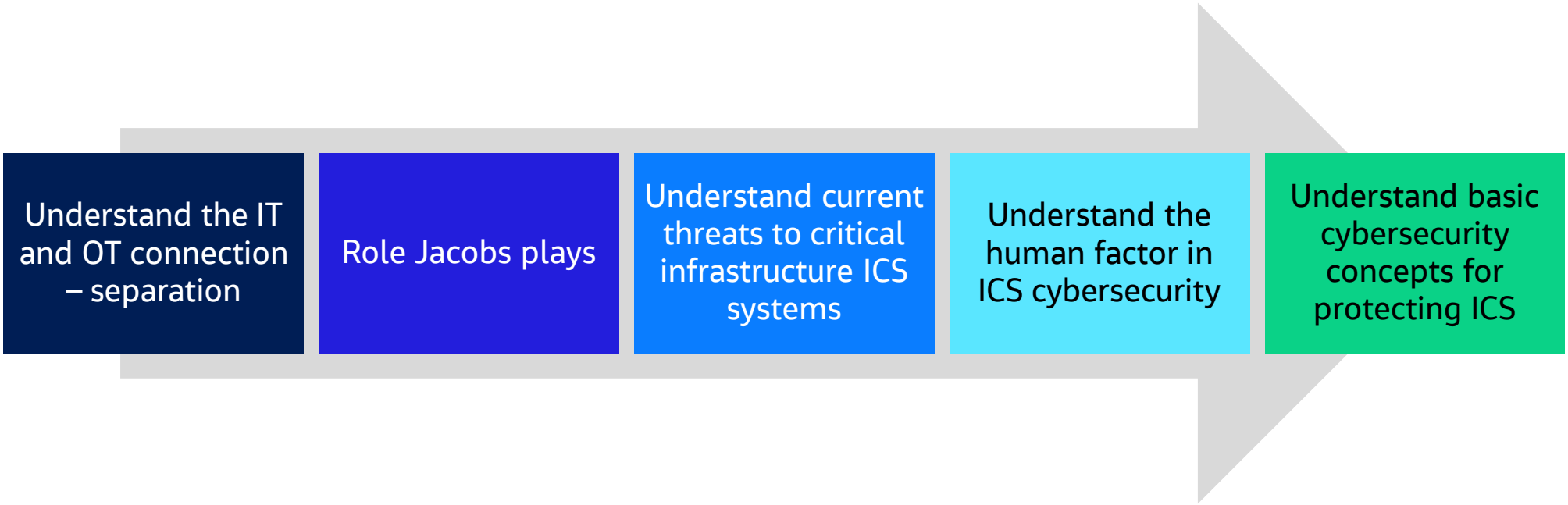
- **Russell Ford**, Jacobs Global Solutions Director for Drinking Water & Reuse
- **Adi Karisik**, Global Technology Leader Operational Technology (Cybersecurity)
- **John Rickermann**, Managing Director, Technical Services Group, Operations Management & Facilities Services

Jacobs Challenging today. Reinventing tomorrow.

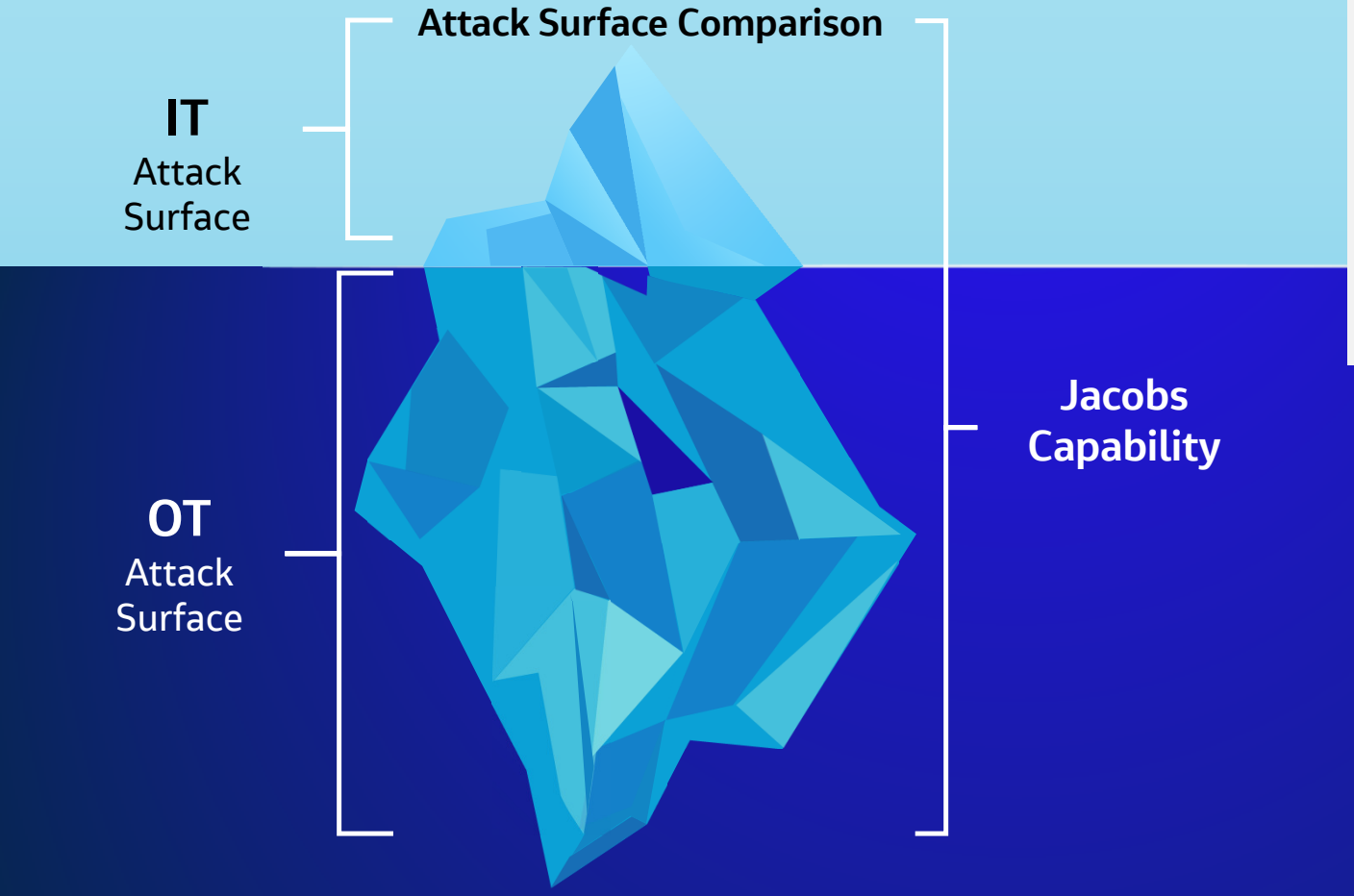
Cybersecurity

Adi Karisik
Global Technology Leader Operational Technology
(Cybersecurity)

What We Will Cover



OT and IT – The Iceberg Principle



Current Cybersecurity Foot-print

- **3,000+** Professionals
- **50** Locations
- **400+** Active Projects
- Compliance Regulations, Industry Frameworks & Agency Guidance

Operational Technology - Definition

Gartner defines Operational Technology as:

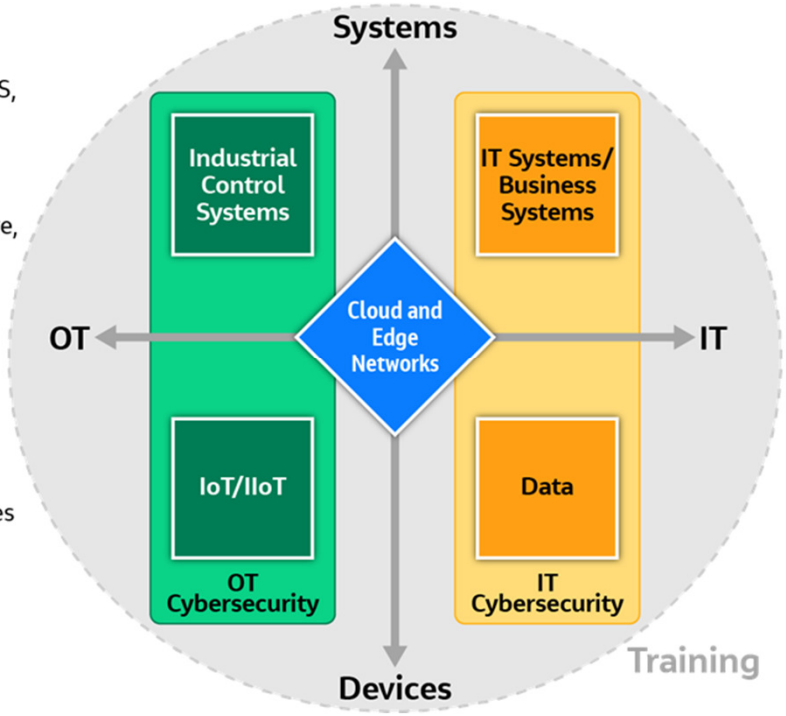
"The practices and technologies used to protect people, assets and information involved in the monitoring and/or control of physical devices, processes and events."

Operational Technology (OT) *also* refers to the practice surrounding IT support for Industrial Control Systems (ICS) or SCADA/DCS

Manage Physical Processes

- Industrial Controllers (PLC, DCS, SCADA) & IO
- Hardened PCs & Servers
- Industrial Networks
- Sensors (Temperature, Pressure, etc.)
- Cameras, Scanners, etc.
- Embedded Systems (Robots, Analyzers, etc.)

- Secure Physical Things and Processes

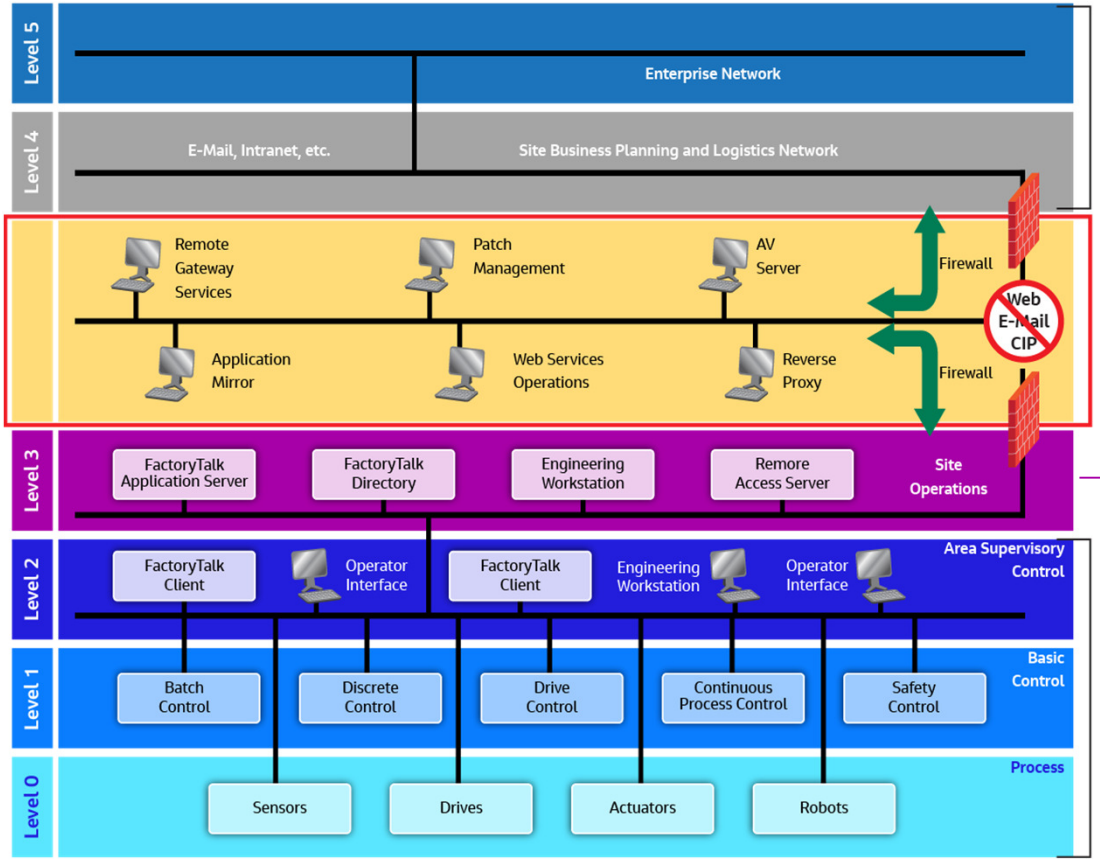


Manage Information

- Secure Data and Business Processes
- Printers
- Web/App/Data/Email Servers
- TCP Networks

- Tablets
- Smart Phones
- Etc.

Purdue Model



Enterprise IT Cybersecurity (Levels 4-5)

Focused on protection of data or information

- Includes protecting data and services across IT infrastructure.
- Associated with Business or Enterprise Systems
- Only deals with IT components, software and communications

DMZ (Levels 3.5)

- Convergence point for IT and OT

OT Cybersecurity (Levels 1.5-3)

Focused on protection of physical processes

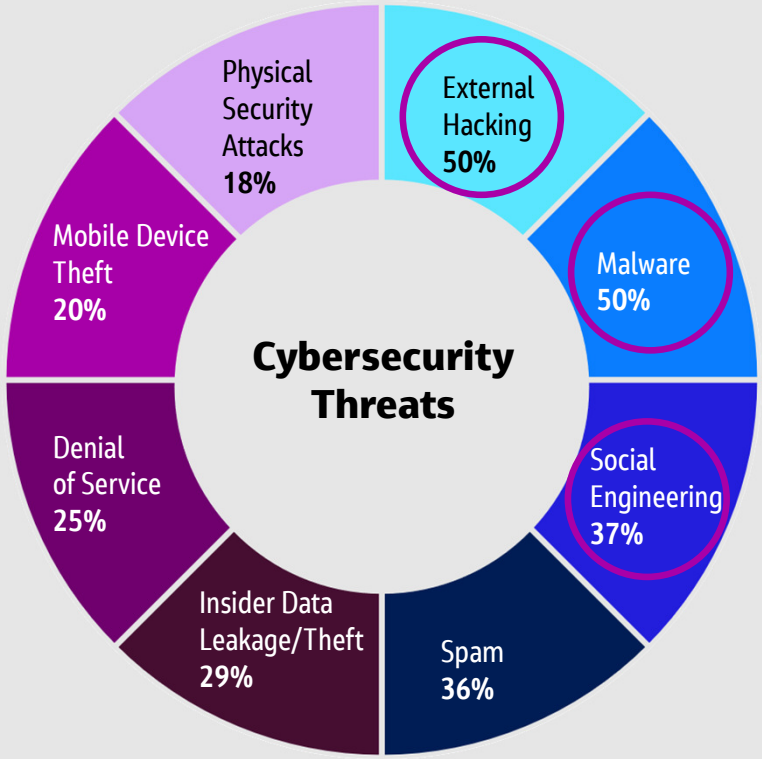
- Includes protecting physical systems, industrial processes, operation of control systems
- Associated with Critical Infrastructure, Energy, Water, Critical Manufacturing, Mining, Chemicals, Commercial Facilities, Dams, Food and Agriculture, Nuclear, Transportation
- Only deals with operational technology components, software and communications (IT type hardware and software in an industrial environment)

SCADA System Design and Integration (Levels 0-1.5)

- **Supervisory control and data acquisition** (SCADA) is a system of software and hardware elements that allows industrial organizations to: … Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software.
- **SCADA** system components and software utilize the foundation of OT infrastructure.

Some Food for Thought

- How do you identify and track your IoT/OT devices today – and know their CVE's?
- How would you know if an adversary is already in your network or has already compromised an unmanaged ICS or IoT device?
- What is your current processes to investigate, remediate and prevent incidents from unmanaged devices?
- How easy is it for your IT and OT people to communicate and solve problems together?
- What happens when your security monitoring vendor does not support a given protocol or device in your environment?



Jacobs Approach

We have a unique approach to securing critical infrastructure:

- We operate over a hundred utilities globally and thus combine the issues/perspective of owner/operator with best technologies and practices available to a systems integrator to provide best cybersecurity protection
- Combine that with our global reach and partnerships and one can get a true picture of our capabilities

Water & Wastewater OM System Controls

John Rickermann

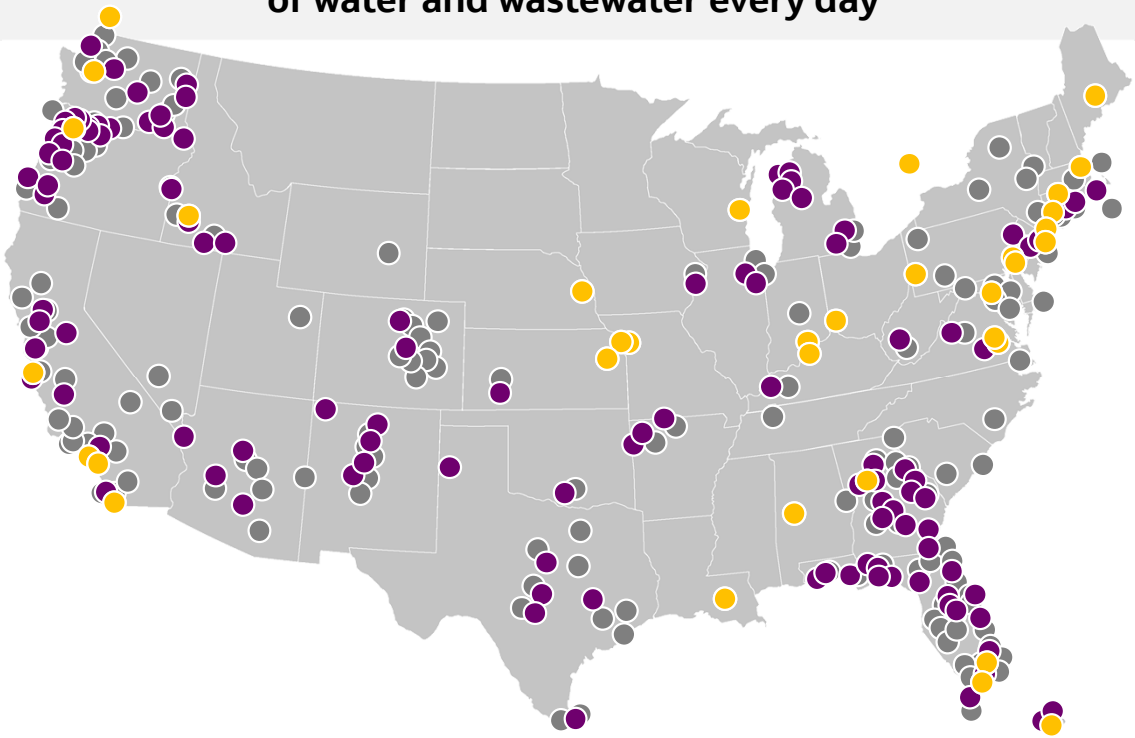
Managing Director, Technical Services Group, Operations Management & Facilities Services

Diversity of Projects, Locations and Requirements

300+
projects

treating **1.1B** gallons
of water and wastewater every day

3,000
O&M staff



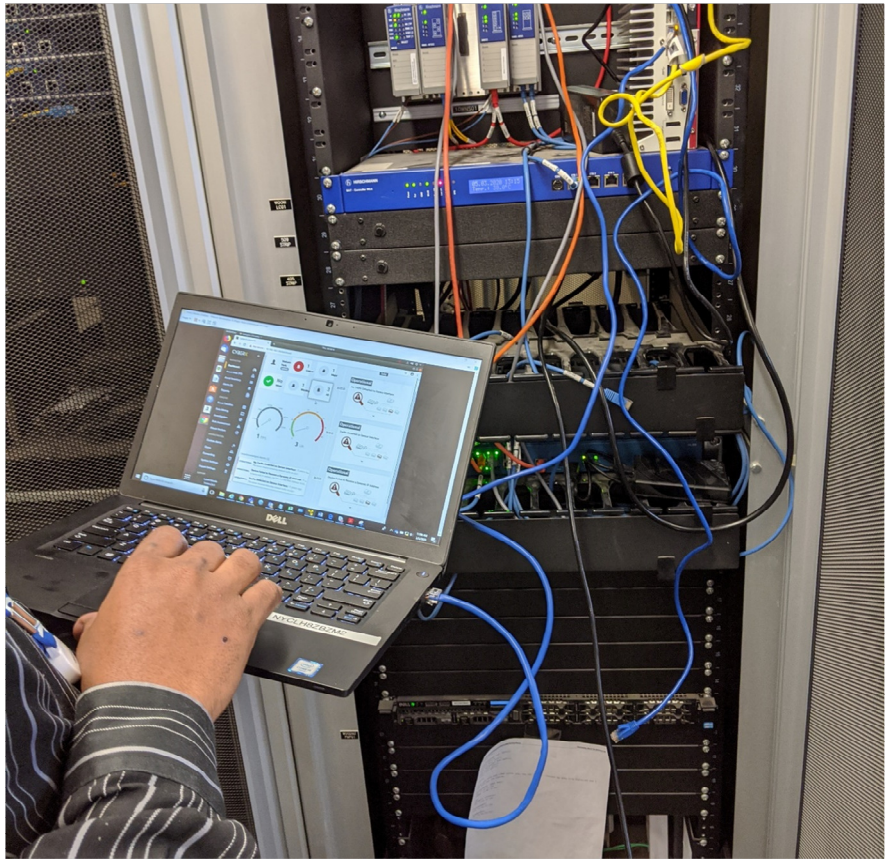
Program Management Long-term O&M contract DB/DBO/O&M projects

Industry Recommended Basic Protections

Industry Recommended Basic Protections

ACTIONS TO PREPARE FOR A CYBER INCIDENT

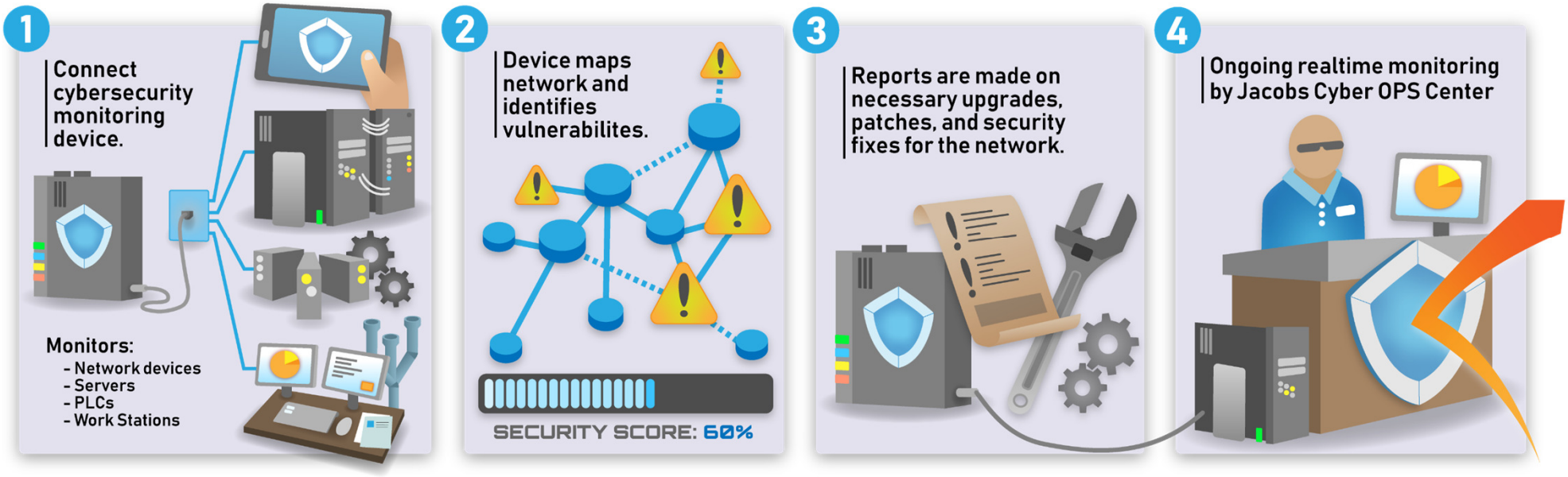
ACTIVITY	CHECKLIST	
☐ Identify and document all critical IT systems; identify entity responsible for operating and maintaining the respective IT system.	☐ SCADA Systems ☐ Operational Databases (Hach WMMS) ☐ Maintenance Connection ☐ Internet/Networks	☐ Geographical Information Systems ☐ Utility Billing and Customer Services System ☐ Utility Website
☐ Identify IT system security Lead.	☐ _____	
☐ Validate cybersecurity practices are in place for each of the critical IT systems above.	☐ Confirmed	
☐ Identify priority points of contact for reporting a cyber security incident and requesting assistance with response and recovery.	☐ Jacobs Management ☐ Client Utility ☐ Local Law Enforcement	☐ State Regulators
☐ Prevent unauthorized physical access to facilities and IT systems	☐ Facilities and IT systems are protected	☐ Changes to facility access are in progress
☐ Define roles and responsibilities of staff during a cyber incident. Train personnel to perform mission critical functions.	☐ Water Plant Operations ☐ Wastewater Plant Operations	☐ Water Storage and Transmission Systems ☐ Wastewater Collection and Pumping Systems



Cyber Audits and Protection

- AWIA requirements for water plants
- CISA and EPA minimum standards
- Periodic audits
- Additional protections
- Firewall
- Supplemental Active Monitoring

Cyber Protection



Protecting Your Assets

Adi Karisik
Global Technology Leader Operational Technology

Why IoT/IIoT/OT Cybersecurity is Now a Board-Level Concern?

Digital transformation & IT/IIoT/OT connectivity have significantly expanded the attack surface

Adversaries are motivated, sophisticated & increasingly destructive

Enterprise SOCs today have virtually no visibility into their IoT/IIoT/OT risk

IoT/IIoT/OT Cyber Risk is a Business Risk

Production downtime

Financial losses

- Top 6 firms impacted by NotPetya lost $129- $870M
- Norsk Hydro lost $71M due to LockerGoga attack

Loss of sensitive intellectual property

Reduced competitive posture

- Manufacturing firms are 8x more likely to be breached for theft of trade secrets than other vertic**als** *(2020 DBIR)*

Safety & environmental incidents

Compliance violations, legal liability & brand impact

- USCG reports port cargo handling equipment compromised via Ryuk
- TRITON attack on safety controllers of petrochemical facility

Example - Why Unmanaged IoT/OT Devices are Soft Targets

- Unseen, unpatched, misconfigured — and “un-agentable”
- Not designed with security in mind
- Weak or default credentials
- Vulnerable open-source components
- IT network monitoring tools blind to specialized industrial protocols

US CISA/NSA Advisory (July 23, 2020)

"Cyber actors have demonstrated their continued willingness to conduct malicious cyber activity against critical infrastructure."
Organizations should create an accurate and detailed OT infrastructure map; use the validated asset inventory to investigate and determine specific risks associated with existing OT devices; and implement a continuous and vigilant system monitoring program with anomaly detection.

ICS Threat Vectors

Nation States

- Intentional attacks, recon, entrenchment

Insider threats

- Intentional attacks and unintentional attacks

Other threats

- Script kiddies, non-intentional damage
- Malware/virus – non-intentional target
- Ransomware – intentional but non-targeted
- Poorly designed systems
- US! We are targets of nation states

Threats to ICS Security: Nation States

Threats to ICS Security: Nation States

Recent Cyber Attacks on U.S Utility Companies Have Been Traced to Iran

Many U.S. utility companies have reported that their data was hacked from a latest wave of sophisticated cyber attacks. According to the New York Times, the Federal officials at US that have been investigating the issue with internet security firms and have claimed hackers are mainly aimed attacks towards major energy producers of the country.

Officials feel that the hack attacks have been brought about to cause catastrophic failure. They have come to a conclusion that the attacks have been traced to Iran by the security experts.

Fraud

As of 23 February 2017, unknown cyber criminal actors compromised a water utility company's SCADA system and downloaded malware, altered identified account settings, and made fraudulent financial transactions from the SCADA system which appeared to be connected the Internet. The actors accessed the SCADA system on five different dates multiple times, and it was unclear how the initial infection occurred.

Insider Attacks – The Human Factor

Insider Attacks are most damaging


The Register®

Data Center Software Networks Security Business Hardware Science Bootnotes Video

Operating Systems Applications Developer Verity Stob

SOFTWARE

Hacker jailed for revenge sewage attacks

Job rejection caused a bit of a stink

By Tony Smith, 31 Oct 2001

Maroochy Shire, Queensland, Australia

Insider threats are most often underestimated and cause the most damage

Maroochy Wastewater

Event: More than 750,000 gallons of untreated sewage intentionally released into parks, rivers, and hotel grounds

Impact: Loss of marine life, public health jeopardized, $200,000 in cleanup and monitoring costs

Specifics: SCADA system had 300 nodes (142 pumping stations) governing sewage and drinking water

- Used OPC ActiveX controls, DNP3, and ModBus protocols
- Used packet radio communications to RTUs
- Used commercially available radios and stolen SCADA software to make laptop appear as a pumping station
- Caused as many as 46 different incidents over a 3-month period (Feb 9 to April 23)

Lessons learned:

- Suspended all access after terminations
- Investigate anomalous system behavior
- Secure radio and wireless transmissions

Ransomware

1. In June 2017, a US water utility company's SCADA computer was infected with BTCWare ransomware variant and encrypted all the SCADA configuration files, logs and reports.
2. The water facility received notification on the infection by a splash screen containing instructions including e-mailing a "qq.com" email using unique identifier to pay a ransom of about USD 5,000.
3. An employee of the water facility emailed the address and received response the next day with a Bitcoin wallet address.
4. The FBI received no information regarding the firewall configuration or internet-connectivity of the network.

ICS Threat Summary

- In today's world no ICS is safe from attacks
- Don’t underestimate the threats
- You need to be aware of cybersecurity practices
  - Free online training from ICS-Computer Emergency Response Team
- Ask for help
- Know your resources
- Avoid human factor attack vectors
- We need to have a security mindset just like our safety mindset

Drivers to Address Cybersecurity in the Water Sector

February 12, 2013 Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience

In response to Presidential Policy Directive 21, DHS issued the National Infrastructure Protection Plan, which provides an updated approach to critical infrastructure security.

February 12, 2013 Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity

"It is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure…"

May 11, 2017 Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

Improve access to classified information, incident communication and coordination, provide incentives, protect supply chain for 13636 Section 9 entities (critical infrastructure)

October 23, 2018 America's Water Infrastructure Act (AWIA)

The law includes components that the resiliency assessments and ERPs must address…..including cybersecurity

Cybersecurity and Infrastructure Security Agency - Act of 2018

Reasons for the Water Sector to use NIST Guidance

- EPA Response to Executive Order 13636

If the voluntary partnership model is not successful in achieving widespread implementation of the Cybersecurity Framework or if warranted by a changing cybersecurity risk profile, the EPA can revisit the option of using general statutory authority to regulate cybersecurity in the Water and Wastewater Systems sector.

Respectfully,

Peter C. Grevatt, Director
Office of Ground Water and Drinking Water

- OSHA objective - Work with Congress to pursue action to remove the Water and Wastewater Treatment Facilities Exemption from CFATS so that security at these facilities can be regulated

- The Tri Chairs CFATS Working Group has recommended Water and Wastewater not be excluded from CFATS

Cybersecurity Guidance

DHS Industrial Control Systems Security Cyber Emergency Response Team (ICS-CERT)	https://ics-cert.us-cert.gov/Recommended-Practices
Critical Infrastructure Security Agency (CISA)	https://ics-cert.us-cert.gov/Standards-and-References
Water Information Sharing and Analysis Center (WaterISAC)	https://www.waterisac.org
NIST Framework for Improving Critical Infrastructure Cybersecurity	https://www.nist.gov/cyberframework
NIST SP 800-82 Guide to Industrial Control Systems Security	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
ISA/IEC 62443	http://www.isa.org/standards

Other NIST Publications / Guidelines

800-37: Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach

http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

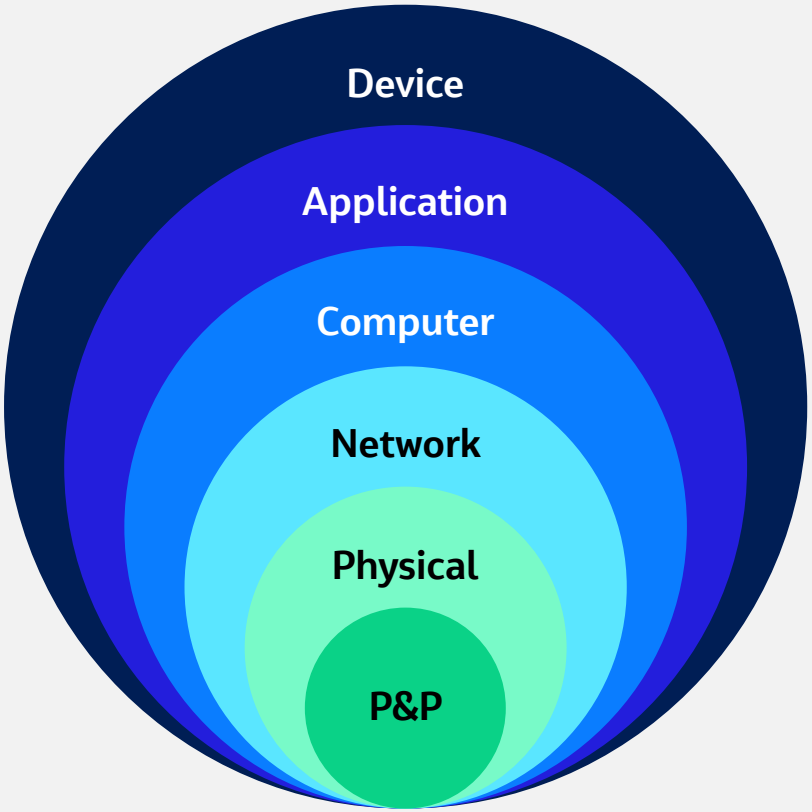
800-37: Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach

http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

800-37: Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach

http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

Defense in Depth



Defense in Depth Strategy Recommendations

- Build a proactive security model
- Adopt standardized countermeasures for Industrial Control Systems
- Keep abreast of Security Standards (NIST, ANSI/ISA 62443 etc.)
- Use the Industry available tools and services DHS CISA CSET, DAR, NAVV, Training AWWA Cybersecurity Guidance & Tool
- Continue building a robust ICS cybersecurity program

Remember Maroochy Shire

- Security via air gap isolation does not work
- Security via obscurity does not work
- It cannot protect against insider attacks and targeted intrusions

System Integrators

Do your integrators know and follow cybersecurity best practice?

Secure system builds

- Are your systems built on shared networks?
  - Interconnected to other networks or internet?
- Connect development systems/laptops to more than one network/project?
- Install anti-virus/malware at the beginning of a system build?
- Are software download hashes checked for authenticity?

Does your SI secure your:

- Block Diagrams?
- Networks Diagrams?
- System Information?
- PLC/PAC Code

Does your SI use the same password on all projects?

Example

Two US power plants infected with malware spread via USB drive

Investigators find no up-to-date antivirus, system backups for control systems.

by **Dan Goodin** - Jan 15 2013, 12:30pm PDT

BLACK HAT NATIONAL SECURITY 52

Richard Webb

Critical control systems inside two US power generation facilities were found infected with computer malware, according to the US Industrial Control Systems Cyber Emergency Response Team.

Both infections were spread by USB drives that were plugged into critical systems used to control power generation equipment, according to the organization's newsletter for October, November, and December of 2012. The authors didn't identify the owners of the facilities and there's no indication the infections resulted in injuries or equipment failures.

Practice System Data Protection

- Secure PLC code
- Secure HMI files
- Secure Project Files
- Secure Network and Block Diagrams

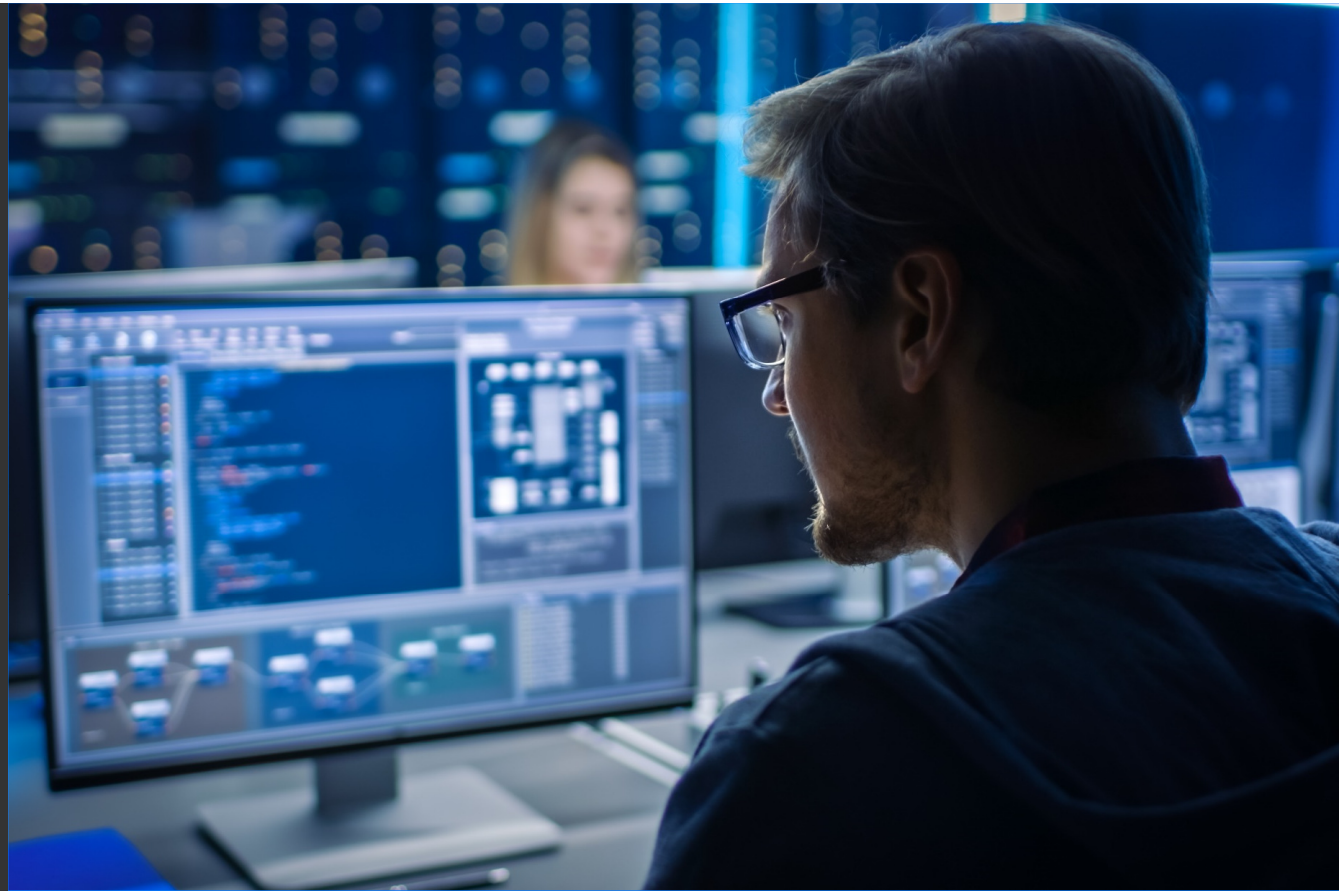
Cybersecurity Best Practice Concepts

- Physical Security
- Network Segregation
- DMZ
- VLAN's
- Active Directory Integration
- Privileged Access Management
- Multi-Factor Authentication (MFA)
- Backups and Disaster Recovery

Physical

Physically Secure:

- Network Equipment
- Server Equipment
- Control Rooms
- PLC's
- Radios
- Use Intrusion Alarms



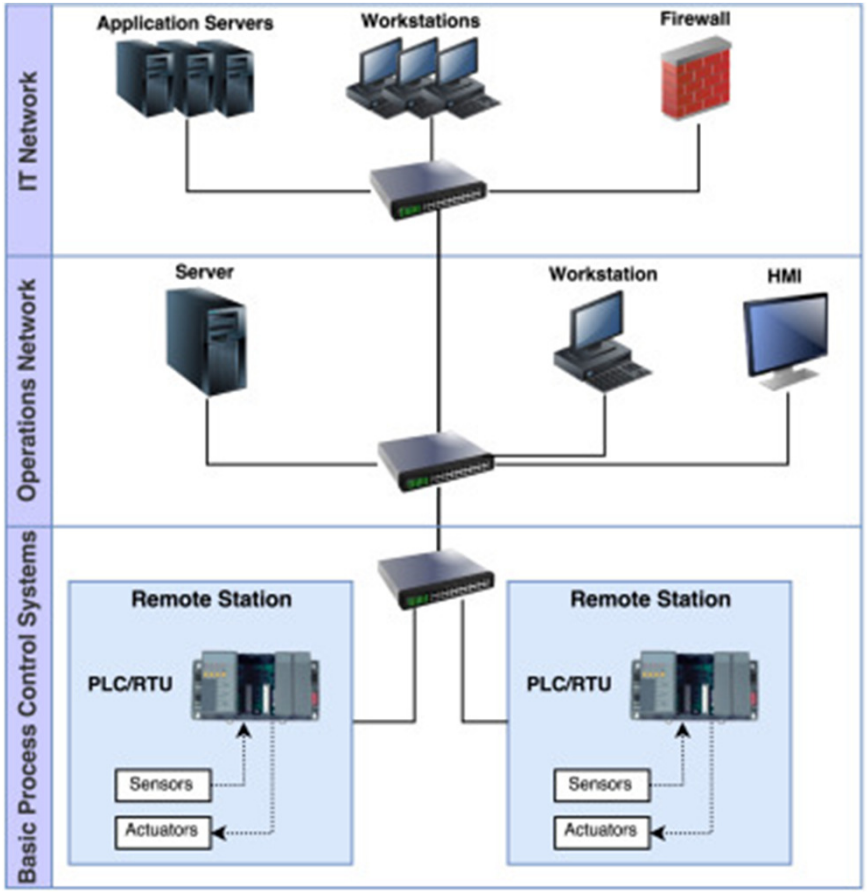
Network Segregation via Firewall

Functions

- Segregate Networks (create Security Zones)
- Inspect and monitor traffic

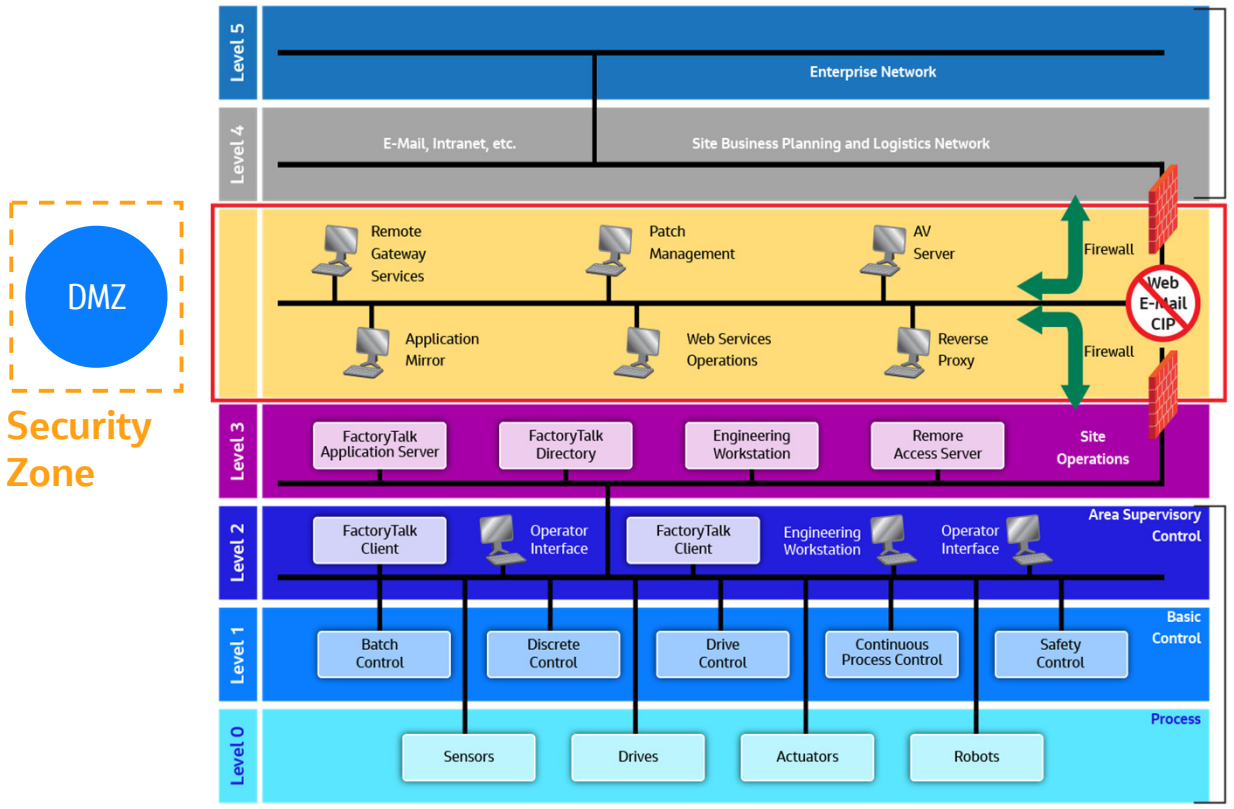
NIST SP 800-82r2 5.1

- "Network segmentation and segregation is one of the most effective architectural concepts that an organization can implement to protect its ICS."



What goes here?

- **NIST SP 800-82 5**
  "Servers containing the data from the ICS that needs to be accessed from the corporate network are put on this network segment."
- **NIST 800-82 5.3.4**
  "If a patch management server, an antivirus server, or other security server is to be used for the control network, it should be located directly on the DMZ."
- **Remote access gateway**



Ancient City of Babylon

Remote Access Management

- NIST SP 800-82r2 5.3 – "Enforce secure authentication of all users seeking to gain access to the ICS network from other security zones."
- "All Firewalls will have logging enabled and will be monitored for traffic flow issues and intrusion detection."
- DHS guidance on remote access for ICS
- Use 2 Factor Authentication (MFA) for all remote access (something you have and something you know or something you are)
- Remote access should be through DMZ only
  - Gateway Server (or PAM)
  - HMI Viewer in the DMZ
- Direct remote access to the ICS is not recommended
  - Smaller projects may require it
  - Use mitigating security controls

Other Network Security Measures

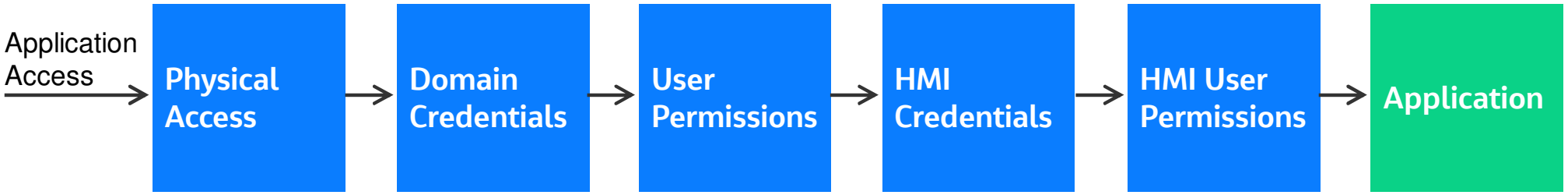
- NIST SP 800-82r2 5.3 - Block all communications with the exception of specifically enabled communications between devices on the unprotected LAN and protected ICS networks. Blocking is based on source and destination IP address pairs, services and ports.

- All Firewalls will have logging enabled and will be monitored for traffic flow issues and intrusion detection.

Application/HMI Security

- No auto logon to workstation
  - Users should use “unique” domain authentication to login to workstations
  - No generic accounts
  - HMI authentication should be enforced
- HMI user permissions should be set
- No Auto Logon HMI’s – It is a BAD idea

Defense in Depth



Backups

- Backup Security
- HMI backups
- PLC code backups
- Server backups
- Workstation backups
- Offsite storage
- Keep backup data secure
  - From deletion
  - From unauthorized access

Disaster Recovery

- Have secure offsite (encrypted) backups that you have verified
- Virtualization makes recovery easier
- Plan for various levels of disaster
  - Hardware failure
  - Application corruption
  - Virus/Malware infection
- Have pre-defined DR plan per NIST SP 800-82

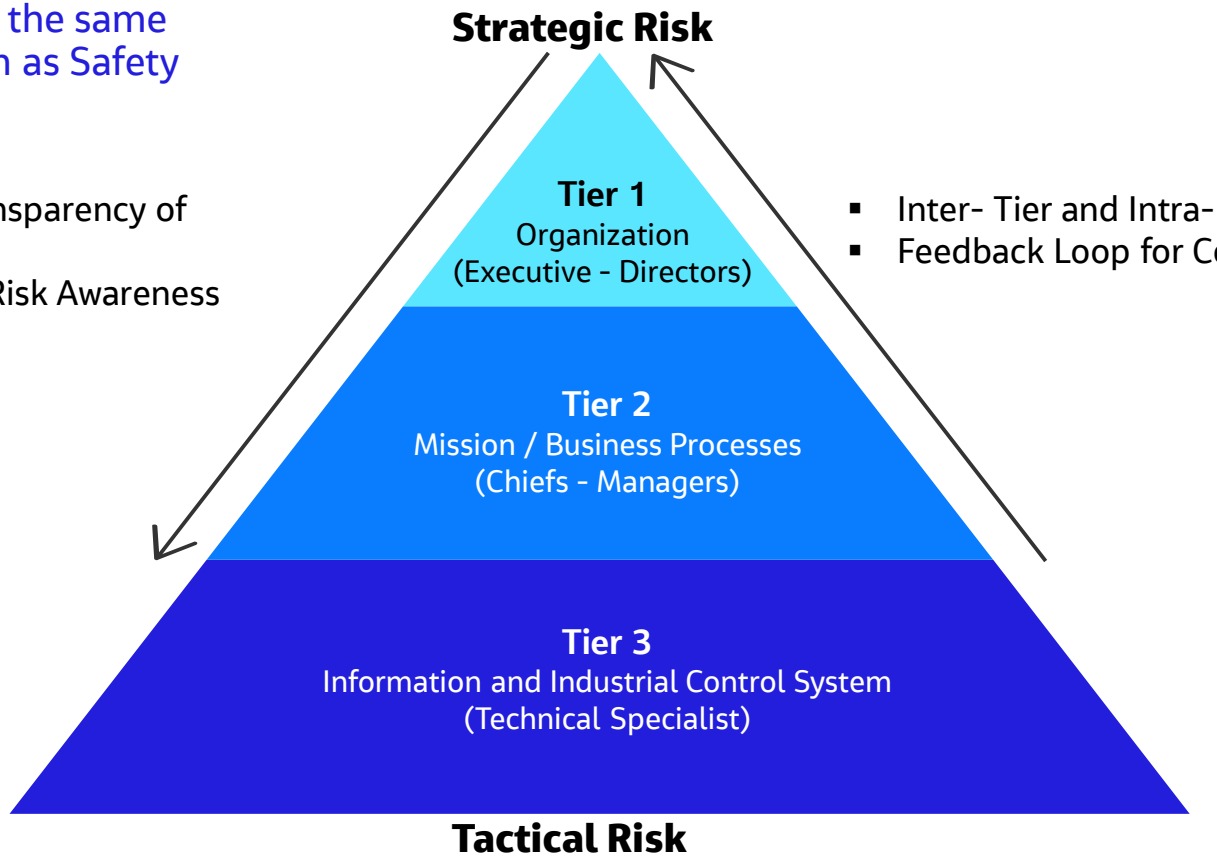
Cyber Resiliency

What Should Water Utilities Focus On	
Operational Efficiency	▪ How do we identify & rapidly eliminate inefficiencies from misconfigured or compromised networks/equipment?
IoT/OT Asset Discovery	▪ What devices do we have & how are they communicating – so we can easily implement better segmentation & zero-trust policies?
Unified IT/OT Security Monitoring & Governance	▪ How do we leverage existing people, training & tools to centralize IT/OT security in our SOCs? ▪ How do we demonstrate to auditors that we have a safety- and security-first environment?
Risk & Vulnerability Management	▪ What are risks to our "crown jewel" type assets ▪ IoT/OT assets — and how do we prioritize mitigation?
Continuous IoT/OT Threat Monitoring, Incident Response & Threat Intelligence	▪ How do we know if we have any IoT/OT threats in our network right now — and how do we quickly respond to them?

Cybersecurity is an Organization–Wide Responsibility

Security should have the same status in organization as Safety

- Traceability and Transparency of Risk-Based Decision
- Organization-Wide Risk Awareness



- Inter- Tier and Intra- Tier Communications
- Feedback Loop for Continuous Improvement

More useful resources

- AWWA Cybersecurity Guidance Tool
- DHS ICS-Cert free online cybersecurity training
- SCADAHacker.com – Great library page
- ICS-CERT
- Operation Cleaver Report
- National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat
- UK Centre for the Protection of National Infrastructure
- ISA 99 – Cost $$

Thank You!

Adi Karisik
Global Technology Leader OT (Cybersecurity)
adi.karisik@jacobs.com

John Rickermann
Managing Director, Technical Services Group, Operations Management & Facilities Services
john.Rickermann@jacobs.com

Jacobs

Questions and Answers

Copyright Notice

Important

The material in this presentation has been prepared by Jacobs®.