



## **Water Information Sharing and Analysis Center**

**Water Sector Monthly Cyber Threat Web Briefing  
August 25, 2021**

# Housekeeping

- This webinar is being recorded.
- The recording and slide deck will be available by tomorrow at [waterisac.org/webcasts](http://waterisac.org/webcasts).
- There will be a Q&A session.

# Presenter

- Jennifer Lyn Walker, WaterISAC

# Fundamentals First Series



## 15 Cybersecurity Fundamentals for Water and Wastewater Utilities

Best Practices to Reduce Exploitable  
Weaknesses and Attacks

2019  
[waterisac.org/fundamentals](http://waterisac.org/fundamentals)

- Expound on each
- Add more OT-specific content
- Map to NIST functions (identify, protect, detect, respond, recover)
- Help less resourced utilities with prioritization

# 15 Cybersecurity Fundamentals for Water and Wastewater Utilities


Download the guide – <https://www.waterisac.org/fundamentals>

1. **Perform Asset Inventories**
2. **Assess Risks**
3. **Minimize Control System Exposure**
4. **User Access Control**
5. **Physical Access**
6. **Cyber-Physical Safety**
7. **Vulnerability Management**
8. **Cybersecurity Culture**
9. **Governance**
10. **Threat Detection**
11. **Business Continuity**
12. **Insider Threats**
13. **Supply Chain Risk**
14. **Smart Device Management**
15. **Information Sharing**

# 1. Perform Asset Inventories

*Maintain an accurate inventory of all OT and IT assets*

**Why it's important: *Imperative for assessing what is at-risk, managing vulnerabilities, and responding to incidents***

- **Start Here** 
- Asset inventory records must be comprehensive and kept current
  - ❑ ditch the spreadsheet
  - ❑ consider incorporating (asking for) SBOMs (Software Bill of Materials) from vendors
- Helps identify unauthorized/rogue/shadow assets
- Discover vulnerable assets before the bad guys exploit them
- Include physical inspections (across all locations)
- Investment now will help avoid paying for it later

## Resources

What is OT/ICS asset management? (Ralph Langner)  
5 Benefits of Asset Inventory Management for OT (Verve Industrial)  
Requiring SBOMs and their Impact on OT (Dale Peterson)  
Get your Stuff Off Search – S.O.S. (CISA)

## 2. Assess Risks

*Perform thorough risk assessments of both OT and IT environments*

**Why it's important: *Identifies risks and vulnerabilities to help prioritize risk control mitigation***

- Required by AWIA > 3300 population served
- Must keep pace with changing environment (cyber threats, new/old devices, new people, processes, procedures) – *once every 5 years is probably not sufficient*
- Factors determining risk severity include, threat (probability/likelihood), vulnerability, consequence (potential impact)

### Resources

Cybersecurity Guidance and Tool (AWWA)

Cyber Resource Hub (CISA)

Vulnerability Self Assessment Tool (EPA)

# 3. Minimize Control System Exposure

*Minimize exposure of control system devices to external networks*

**Why it's important: *Protects the control system environment from "hostile" networks***

- "Air gap"
- Unidirectional communications (one-way data diodes)
- ICS DMZ
- Jump box
- Network segmentation
- Restrictive procedures
- Secure remote access

## Resources

Recommended Cybersecurity Practices for Industrial Control Systems (CISA)

Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies (CISA)

Is the Purdue Model Still Relevant (David Greenfield)



# Resources

- <https://www.langner.com/2020/09/what-is-ot-ics-asset-management/>
- <https://verveindustrial.com/resources/blog/5-benefits-of-asset-inventory-management-for-ot/>
- <https://dale-peterson.com/2021/04/27/requiring-sboms-and-their-impact-on-ot/>
- <https://www.cisa.gov/publication/stuff-off-search>
- <https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance>
- <https://www.cisa.gov/cyber-resource-hub>
- <https://vsat.epa.gov/vsat/>
- [https://www.waterisac.org/system/files/articles/Cybersecurity\\_Best\\_Practices\\_for\\_Industrial\\_Control\\_Systems.pdf](https://www.waterisac.org/system/files/articles/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf)
- [https://us-cert.cisa.gov/sites/default/files/recommended\\_practices/NCCIC\\_ICS-CERT\\_Defense\\_in\\_Depth\\_2016\\_S508C.pdf](https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf)
- <https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant>

# Cybersecurity Updates

Threats and Vulnerabilities | Reports |  
Tips and Resources | Analyst Spotlight

# Threats and Vulnerabilities

## April 29, 2021

- Microsoft identifies “BadAlloc” vulnerability, issues advisory
- CISA publishes ICS Advisory ICSA-21-119-04, “Multiple RTOS”

## May 24, 2021

- CISA publishes Update B to Multiple RTOS alert
- States its impact on RTOS

## August 17, 2021

- BlackBerry public acknowledgement
- CISA issues Alert AA21-229A
- States its impact on RTOS
- CISA publishes Update C to Multiple RTOS alert, adding BlackBerry QNX

### About the Vulnerability

CVE-2021-22156

Originally disclosed by Microsoft in April 2021

No active exploitation known

Software updates developed

### Industries Impacted

Automotive, Transportation, Healthcare, Energy, Defense

### Open-Source Advisories

CISA

BlackBerry

Microsoft

ICS Advisory (ICSA-21-119-04)

# Threats and Vulnerabilities

## Potential Outcomes

- Vulnerability exists in BlackBerry QNX RTOS
  - Used in a wide range of ICS
- Exploitation could lead to
  - Denial of Service (DoS)
  - Arbitrary Code Execution
  - Deny system availability, exfiltrate data
  - Seize control of ICS components

## Recommendations

- Patch affected products
- Basic cybersecurity hygiene practices
  - Limit access to RTOS
  - Network segmentation best practices
  - Vulnerability scanning/intrusion detecting

## About the Vulnerability

CVE-2021-22156

Originally disclosed by Microsoft in April 2021

No active exploitation known

Software updates developed

## Industries Impacted

Automotive, Transportation, Healthcare, Energy, Defense

## Open-Source Advisories

CISA

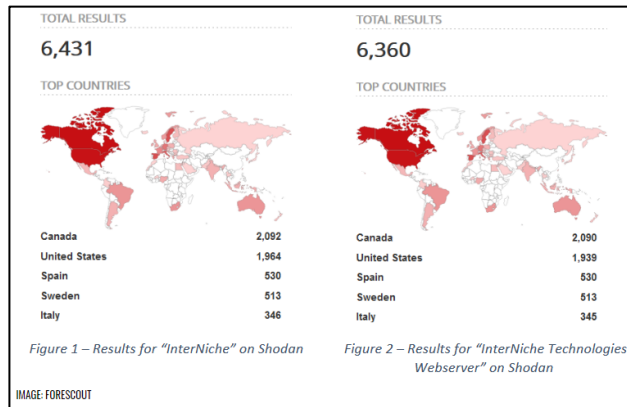
BlackBerry

Microsoft

ICS Advisory (ICSA-21-119-04)

# Reports

- INFRA:HALT Vulnerabilities Affect OT Devices from More than 200 Vendors ([Forescout](#))



- Lessons Learned from Examining More than a Decade of Public ICS/OT Exploits ([Dragos](#))
- Threat Landscape for Supply Chain Attacks ([ENISA](#))
- Saudi Aramco Data Breach and Extortion ([Flashpoint](#))

# Tips and Resources

- “Get Your Stuff Off Search” ([CISA](#))

How-to Guide:  
**Stuff Off Shodan**

How-to Guide:  
**Stuff Off Censys.io**

How-to Guide:  
**Stuff Off Thingful**

- Cybersecurity Workforce Training Guide ([CISA](#))
- The Business Case for Security ([CISA](#))
- Securing Devices while in Public ([NSA](#))

# Analyst Spotlight

- Some Vulnerabilities Don't Go Out of Style ([WaterISAC](#))
- Passwords and Predictability ([WaterISAC](#))

Ever heard of a 'BoardingSharkMan'?

We hadn't either, that's why it would make a good password. Choose three random words, the dafter the better! [nscs.gov.uk/cyberaware/hom...](https://nscs.gov.uk/cyberaware/home) 🟢 #CyberAware



Create a strong password using 3 random words.

The dafter the better.

 National Cyber Security Centre  
a part of GCHQ

 Cyber Aware

# Upcoming WaterISAC Events

- Monthly Water Sector Cyber Threat Briefing
  - Wednesday, September 22, 2021; 2:00 – 3:00 PM ET

Register on WaterISAC's Events webpage:

<https://www.waterisac.org/events>



# Thank You

WaterISAC Contact Information:

**1-866-H2O-ISAC**

**Michael Arceneaux**

Managing Director

[arceneaux@waterisac.org](mailto:arceneaux@waterisac.org)

**Kaitlyn Palatucci**

Membership Engagement Director

[palatucci@waterisac.org](mailto:palatucci@waterisac.org)

**Charles Egli**

Preparedness and Response Director

[egli@waterisac.org](mailto:egli@waterisac.org)

**Jennifer Lyn Walker**

Infrastructure Cyber Defense Director

[walker@waterisac.org](mailto:walker@waterisac.org)