WEF MA – cybersecurity fundamentals
Words: 829

Headline: Cybersecurity Fundamentals Guide for Water and Wastewater Utilities Now Available

Michael Arceneaux and Jennifer Lyn Walker

Water and wastewater utilities provide critical lifeline services to their communities and their regions. Supporting these vitally important functions requires secure information technology (IT) and operational technology (OT), yet the sector's IT and OT networks continue to face an onslaught of threats from cyber criminals, nation states, and others.

To support the sector in its cybersecurity goals, and in response to the continually evolving threats, WaterISAC, the Water Information Sharing and Analysis Center, has just published a newly updated resource: *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*.

The updated guide contains dozens of best practices, grouped into 15 main categories, that water and wastewater systems can implement to reduce security risks to their IT and OT systems. Each recommendation is accompanied by links to corresponding technical resources. In sum, the guide connects users to the information and tools needed to take a dive deep into this important issue.

Here is a summary of the 15 fundamentals.

- **Perform asset inventories.** You can only protect what you know about. Knowing your environment is a basic requirement of a sound cybersecurity program.
- **Assess risks.** Once assets inventories are completed, OT and IT risk should be assessed, considering the likelihood a threat will occur and the degree of impact the threat will cause to the organization.
- **Minimize control system exposure.** Protect the control system environment from outside, untrusted networks. This involves network segmentation, traffic restrictions, and encrypted communications.
- **Enforce user access controls.** Users on a network should have no more access than they need to do their jobs. Apply role-based access controls and the principle of least privilege, including limited use of administrator rights to prevent users from accessing systems and files they are not authorized to access.
- **Safeguard from unauthorized physical access.** If an adversary can gain physical access to your equipment, they can compromise it. Non-technical, physical security controls can restrict physical access to IT and OT environments.
- **Install independent cyber and physical safety systems.** Cyber-attacks can result in physical effects. To protect critical assets from such "blended" threats, utilities should consider non-digital engineering solutions such as independent cyber and physical safety systems.
- **Embrace vulnerability management.** Largely informed by asset inventory and risk assessments, vulnerability management involves the need to identify and remediate cybersecurity gaps and vulnerabilities before the bad guys exploit them.
- **Create a cybersecurity culture.** Cybersecurity is everyone's responsibility, the break room to the boardroom. Effective cybersecurity starts at the top; to affect positive behavioral

changes, involve every executive, board member, and employee in cybersecurity awareness and training.

- **Develop and enforce cybersecurity policies and procedures (Governance).** Create, disseminate, and operationalize clear and actionable organizational policies and procedures regarding cybersecurity expectations. The fundamentals in this guide can be used to begin developing policies that are most relevant to each organization.
- **Implement threat detection and monitoring.** You will not find it if you are not looking. The importance of configuring detailed logging and reviewing system logs to detect active threats in your environment cannot be overstated.
- **Plan for incidents, emergencies, and disasters.** Plan ahead for maintaining business continuity and resilience. Emergency response plans (ERPs) will be required by America's Water Infrastructure Act (AWIA) beginning in 2020.
- **Tackle insider threats.** The insider threat is a people problem, not a technology problem; however, not all insider threats are malicious. Mitigate this organizational-level threat by understanding behavioral indicators that predicate an insider threat and apply appropriate training and technology controls to deter an incident.
- **Secure the supply chain.** The supply chain/vendor relationship is a common threat vector for cyber-attacks and must be intentionally managed through security and vulnerability testing and risk assessments.
- **Address all smart devices.** When unsecured internet of things (IoT) and mobile devices are connected to networks, they create holes (often to the Internet) that may not have previously existed. Cisco's *2018 Annual Cybersecurity Report* states that few organizations view IoT as an imminent threat, yet adversaries are exploiting weaknesses in connected devices to gain access to industrial control systems that support critical infrastructure.
- **Participate in information sharing and collaboration communities.** Share information with others. Utilities can learn from each another by getting involved in WaterISAC, InfraGard, and similar communities. Cyber-mature utilities can significantly help the community and sector by sharing their experiences.

About WaterISAC

WaterISAC is a nonprofit water and wastewater sector organization dedicated to protecting sector utilities from all hazards. WaterISAC disseminates threat advisories, reports, and mitigation resources to help utilities prevent cyber and physical security incidents and to recover from disasters.

WaterISAC draws information from federal and state law enforcement and many private sector sources to produce products that are relevant to the water and wastewater sector.

Membership, including a free 60-day trial, is open to utilities, consulting firms, sector associations and state agencies. More information is available at www.waterisac.org.

Michael Arceneaux *is WaterISAC's managing director and* ***Jennifer Lyn Walker*** *is WaterISAC's cybersecurity risk analyst.*