Van Ness Feldman LLP
vnf.com

WaterISAC Releases Broader Cybersecurity Guidelines for Water & Waste Water Utilities

JULY 29, 2019

Gwen Keyes Fleming and T.C. Richmond

The Water Information Sharing and Analysis Center (WaterISAC or Center) has released its "Fifteen Cybersecurity Fundamentals for Water and Wastewater Utilities" (Fundamentals), which is a non-exhaustive list of best practice measures for utilities to reduce their vulnerability to cyberattacks. The fundamental provisions range from strengthening physical barriers and technological monitoring to social planning and workplace strategies. While these fifteen Cybersecurity Fundamentals are similar to the ten Basic Cybersecurity Measures of 2010, they offer more in-depth planning and a broader scope of coverage.

These new Fundamentals will be useful for any water utility developing or updating the requisite risk and resilience assessments and emergency response plans under America's Water Infrastructure Act. (See EPA Issues New Emergency Response Requirements for Community Water Systems.) In addition, as "best practices," the Fundamentals may be referenced by courts, regulators, funders, insurers and claimants in the event a utility experiences a cyber related breach or attack.

Background

The WaterISAC is a non-profit organization governed by water and wastewater utility managers and state drinking water administrators and operated by the Association of Metropolitan Water Agencies. Since 2002 it has provided information and tools to help utilities, agencies, and firms in the water and wastewater sector keep their information technology (IT) and operational technology (OT) functions secure. The Center provides data analysis and resources to its members so they can increase resilience, better respond to threats, and mitigate damage. It is the only resource in the water and wastewater sector to provide comprehensive information for all-threats security. In 2010 the WaterISAC issued a report focused on defending against cyberattacks through basic measures. Most of the 2010 measures are incorporated into the "Fundamental Four" of the new 2019 report, including password security, network segmentation, assessing devices and implementing role-based access control (RBAC), and using virtual private networks (VPNs). Other areas that were addressed in 2010 include policy development for mobile devices, developing cybersecurity incident response plans, installing auto-updates to keep systems and software current, and avoiding suspicious phone calls or emails.

2019 New Cybersecurity Fundamentals

In comparison to the 2010 measures, the WaterISAC's new measures encompass a wide-range of methods to ensure system reliability. Methods include enacting barriers and establishing asset inventories, limiting network access by means of increased password protection and minimized access points, and implementing policies and procedures to ensure that employees receive smart device training. The Fundamentals can be grouped into five categories, four of which track the National Institute of Standards and Technology (NIST) Cybersecurity Framework which has been lauded as the premier standard for implementing sound cybersecurity measures. We provide a summary below:

1. IDENTIFY - Fundamentals 1, 2, 12, 13 and 14

The most basic principle of cybersecurity is to perform ongoing asset inventories and physical inspections, in addition to keeping an updated diagram of network connections. After performing asset inventories, it is essential to establish processes for regular and thorough risk assessments. Since the behaviors of employees, vendors, contractors, and consultants all pose risks, companies should manage both insider threats and potential supply chain compromises. Thus, checks on background and security, as well as establishing required behaviors applicable to the entire team are essential. Lastly, all connected devices pose risks if they are not carefully managed. All smart devices should be included in risk management strategies and all employees who receive such devices should be trained.

2. **PROTECT – Fundamentals 3, 5 and 6**

Companies should minimize control system exposure because a lack of boundary protections for IT networks, Bluetooth communications, and other short-range connections may pose potential threats. Physical barriers should be put in place to keep information in and attackers out. This may include physical fences and barriers, secure control rooms, and limited access to information storage devices. Non-disclosure agreements and background checks may also be used to ensure employee integrity. Additionally, blocking physical access points and installing independent cyber-physical safety systems prevent access to equipment and limit the risk of compromise.

3. **DETECT – Fundamental 10**

Creating a security operations center (SOC) enables organizations to proactively detect and monitor potential threats. SOC data should be logged and routine audits should be conducted to ensure efficient monitoring.

4. **RESPOND – Fundamental 11**

Response plans and disaster recovery plans are critical to an organization's success and ability to overcome major challenges. Threat detection (Fundamental 10) is essential to properly address the scope of damage and accurately respond. A plan must be in place before any compromise occurs. This includes having an on-site backup generator and cybersecurity insurance as a tool to improve a company's resilience and ability to manage breach expenses.

5. **GOVERNANCE – Fundamentals 4, 7, 8, 9 and 15**

Embracing vulnerability management and creating a cybersecurity culture requires that a company develop and enforce cybersecurity policies and procedures. Companies should enforce user access controls including RBAC, password hygiene, secure remote access, and disabling unnecessary access, as a means of effectively minimizing user-based risks. Companies should also recognize that managing vulnerabilities is an ongoing process similar to asset inventory (Fundamental 1) and risk assessment (Fundamental 2). All staff members are responsible for maintaining overall cybersecurity, so general training sessions should be encouraged. Firms are commonly elevating cybersecurity needs by incorporating the role of Chief Security Officer (CSO) or Chief Information Security Officer (CISO) into their governance and C-Suite leadership structure.

Lastly, companies should participate in information sharing and collaborative communities. Water and wastewater utilities face similar cybersecurity threats and therefore can benefit through a collaborative framework. WaterISAC provides a place to share ideas, report issues, and provide input to others in the water and wastewater sector.

FOR MORE INFORMATION

Please contact Gwen Keyes Fleming or T.C. Richmond in Van Ness Feldman's Cybersecurity & Emerging Technologies practice group for additional information related to these guidelines. Summer Associate, Jennifer Wright also contributed to this issue alert.

Follow us on Twitter @VanNessFeldman

This document has been prepared by Van Ness Feldman for informational purposes only and is not a legal opinion, does not provide legal advice for any purpose, and neither creates nor constitutes evidence of an attorney-client relationship.