FRWA Comments on Hyper Attack on Central Florida Water System

As everyone in the Water Industry has been made aware, we have had a hacker attack on a water system in Central Florida. What makes this particular attack so concerning and "an exception to the norm" is that it was not a "Ransomware" which has become increasingly successful. Such attacks have become more of a copy-cat occurrence in our business, however this particular incident was one of greater malicious intent. The hacker intended to increase the Sodium Hydroxide levels by manipulating the SCADA system software. This manipulation had the potential effort to change water quality in the City by the Utility.

This was an alarming incident because the possible victims in this scenario appear to have been selected arbitrarily through remote interaction with the Utility's SCADA system. Fortunately this was a limited impact operation. The intrusion did not result in damage or injury to public health. Many Utilities have processes which are designed to incorporate safety mechanisms which prevent unexpected modifications. While this incident was not particularly complex, It highlights the need to strengthen the cybersecurity capabilities across the water and wastewater industry and to other critical infrastructure sectors.

The Florida Department of Environmental Protection and Florida Rural Water Association have been involved in providing a Risk and Resilience Vulnerability Assessment program to the Water Utility industry. Florida Rural Water Association has offered the service for just over two years in an effort to increase awareness and to share the importance of cyber security protections. We feel that this joint training program, coupled with your Utility Operators, is the best educational tool that can be offered to address the problems associated to the computer hackers of water systems and wastewater systems throughout the state. We are promoting a program that is providing affordable steps and measures to protect systems from computer related, remote operations by outsiders through the SCADA and connected systems.

The number one priority is to train and educate your employees in Security awareness. Situations where hackers are exploiting the users' lack of training and knowledge by phishing attempts that encourage them to open malicious word document attachments or enable macros are now common. Once the user opens the attachment or clicks the "Enable Content", the malicious application can download and start the attack process. Along with the extensive assessments addressed in the IT section of the Risk and Resilience Vulnerability Assessment program, the following three step recommendation is provided for all IT Department managers to adhere to:

1. Perform a penetration test to ensure that the perimeter of the network is secure. Any remote access programs should incorporate safeguards such as strong password protection using randomly generated passwords or other such steps to close the loop.
2. Ensure proper security awareness training for every employee as part of an ongoing training program.
3. Most critical of all is to ensure that data is protected with more than just a single backup mechanism. It is best to have a redundant backup system in place and one that is encrypting and storing backup offsite. For data that is critical, never rely on a single means of recovery.

FRWA encourages you to take affordable and appropriate steps within your budget to reduce vulnerabilities, including increased cyber-security threats. We want to make sure curious hackers are unable to breach their local water utility's computers and security systems. With the current challenges we are facing, the public's eyes are on our industry.

Fortunately, observant employees and security precautions worked at Oldsmar. However we encourage you to take steps now to add additional protection. Increase your security and cybersecurity and provide assurance to your customers and public that you are taking steps to protect them without increasing their utility rates.

FRWA provides a no cost, extensive review process to minimize such exposures and risk of hackers accessing your Utility. Please contact us at any time to provide a partnership assessment of cyber security protection at your Utility.