Volume 9, Issue 2
Winter 2021

Regional Water Cooperative of Pierce County

The Tap

INSIDE THIS ISSUE:

Camano Water Association
City of Bonney Lake
City of Fife
City of Milton
City of Pacific
City of Puyallup
City of Roy
City of Sumner
Covington Water District
Firgrove Mutual
Fox Island Mutual
Fruitland Mutual
Graham Hill Mutual
Lake Josephine Riviera
Lakewood Water District
Mt. View-Edgewood Water
Parkland Light &Water
Peninsula Light Co.
Pierce County Planning and Public Works
Public Utility Dist. No. 1 of Thurston County
Spanaway Water
Summit Water & Supply
Tacoma Water
Town of Steilacoom
Valley Water District
Washington Water Service

Is Your Utility Well-Protected Against a Possible Cyber Attack?

Last year, our customer billing vendor was a victim of ransomware attack. Our District took a very proactive approach in notifying our customers and ensuring open communication regarding the extent of the situation that occurred with the vendor. An IT forensic audit was conducted, and it determined that none of our customer information or data was compromised, thank goodness! We were then able to correspond with our customers to assure them with certainty that their information was not accessed. But this example highlights the issues facing utilities on a lot of different fronts. Plus, during the recent situation in Oldsmar, Florida, a malicious actor gained remote access to the utility's SCADA system and attempted to elevate levels of a certain chemical to a point where it could put the public at risk of being poisoned.

Cyber risk is a serious threat, and it is critical for your utility to make cybersecurity a top priority. These attacks are happening almost daily. Drinking water and wastewater systems not only manage sensitive personal data but they also operate process systems that are essential to day-to-day operations. The federal government has labeled the water sector as the weakest link in the possibility of cybersecurity breaches in comparison to other utility sectors. If your utility does not take the proper steps to mitigate the risk of a Cybersecurity event, it will happen, it's just a matter of time before it does.

The growth of the Internet, and more specifically the industrial "Internet of Things," has led to a greater efficiency in leveraging data to optimize utility operation and processes. This also includes employees with smart phones, tablets, and laptops that allow

CONTINUED ON PAGE 2

Is Your Utility Well-Protected…

CONTINUED FROM PAGE 1

for remotely accessing, monitoring, and managing the system. Most, if not all, utility employees have computers that support some level of Internet connectivity for business purposes, like email. This may or may not include the computers that run Supervisory Control and Data Acquisition (SCADA). Everyone is at risk of clicking on something that has a virus. This can expose a utility's business and operating system to those bad actors who can financially and/or operationally cripple a utility.

Getting cybersecurity right is not an easy issue especially when it comes to convincing Boards, Councils, or Commissioners of the need to invest in Cybersecurity. At a recent AWWA Board meeting I attended in October, I heard that there are discussions within the federal government that if water and wastewater utilities don't enact cybersecurity measures or set up some form of standards for utilities to go by, then the government will. The Board and the Water Utility Council are trying to put forth information and recommendations to help utilities, as well as provide input to the federal government on the need for utilities to enact security systems that help ensure protections for water and wastewater.

Utilities, regardless of the size, must take proactive steps to ensure that there is a plan, a program, and a process in place to prevent, detect, and respond to cyber threats. It is essential to prevent not only a serious repercussion from a cybersecurity attack but also the related reputational harm to the impacted utility that is experienced by way of reduced customer confidence.

I was really pleased to hear how seriously and aggressively AWWA is taking this issue in helping utilities to manage the serious threats. AWWA has set up a cybersecurity guidance and assessment tool at (www.awwa.org/cybersecurity), which is free, available online, and can be used to evaluate individual water and wastewater systems. These resources are developed and issued by the National Institute of Standards and Technology and the United States Department of Homeland Security.

In the not-too-distant future AWWA will be sharing more information and ways to help your utility and you as operators and supervisors with how to further make the case to elected officials and governing bodies that investments into cybersecurity protection levels are necessary to ensure the ability to serve your customers.

CONTINUED ON PAGE 3

Is Your Utility Well-Protected…

CONTINUED FROM PAGE 2

While your utility develops its Cyber Security plan, there are positive steps your utility can take to protect your networks that won't break the bank to implement. This is not an exhaustive list and should not be considered as a complete Cyber Security solution. Each utility and network is unique and should be evaluated by a qualified technology professional for risk assessment and mitigation.

- Train your employees to identify potentially malicious email and text messages. Most breaches and ransomware events are the result of an end user falling victim to a socially engineered message that fooled them in to clicking on a link or attachment that consequently installed malware that in turn led to a Cyber Security event. The Cyber Security event that took out our District's customer billing vendor was the direct result of a vendor employee opening a malicious email. There are plenty of free training resources available online to assist you in implementing a training program. If you currently carry Cyber Liability insurance, your insurance carrier or broker may already have a training program available at no additional cost.
- Implement Multi-Factor Authentication (MFA) on all supported platforms. If your utility uses Office365 or Google Apps this is relatively simple and inexpensive. This step will force an additional authentication step beyond the traditional username and password to access your utilities resources. Usually in the form of a texted code or use of an authenticator app on a mobile device. If you are unable to implement MFA, ensure you have a password policy that ensures complex passwords and frequent password rotation.
- Install security patches on your computers, servers, Network Infrastructure, IoT, and mobile devices whenever possible. Unpatched systems are a serious risk. Patching known exploits reduces the risk of a Cyber Security event occurring through a known exploit. Schedule regular patching of your technology resources.
- Change the default password on all network enabled devices (Printers, Wi-Fi Routers, Network Switches and Routers, Cameras, Payment Kiosks, Etc.). If you have a network enabled device, the default password for this device can be found online.
- Install and keep up to date a reputable Anti-Malware solution for your utility. Most computers have some sort of Anti-Malware solution installed out of the box. In most cases this included solution is already out of date before you have turned on the new computer for the first time. It is critical that you update your Anti-Malware solutions regularly. If you are using Windows Defender as your preferred Anti-Malware solution, these updates are installed through

CONTINUED ON PAGE 4

Is Your Utility Well-Protected…

CONTINUED FROM PAGE 3

Windows Update and again highlight why it is critical to load security updates regularly.

- Isolate your Operations Technology Network (SCADA) from your Information Technology Network. This protects your SCADA system in the event your production network is compromised. If your OT and IT networks currently co-exist on a single network, this can be a complex undertaking that should be planned and performed by a qualified technology professional
- Update, monitor, and regularly test your utility's firewall. If you are using a residential class Router or ISP (Internet Service Provider) provided router to protect your utility's network from external intrusion you are at an increased risk of an external breach. A properly patched and configured business class firewall should provide an intrusion detection service and block undesirable network traffic from entering your network. Intrusion testing and scanning should be performed monthly and whenever a firewall configuration change has occurred. There are several relatively inexpensive network penetration testing and scanning services available online.

As mentioned above, these recommendations do not, in whole or in part, constitute a complete Cyber Security plan. They are simply a small part of the minimum steps that should be considered to protect your utility's technology resources. Cyber Security is a very reactive discipline. Malicious actors are constantly searching for new methods to fool you and your employee's or breach your perimeter networks. Prepare and plan as though you are certain you will experience a breach because the chances are that your utility will.

Randy Black GM and Christian Fast IT Manager

Winter Morning Poem

Winter is the king of showmen,
Turning tree stumps into snow men,
And houses into birthday cakes,
And spreading sugar over lakes.

Smooth and clean and frosty white,
The world looks good enough to bite.
That's the season to be young
Catching snowflakes on your tongue.

Snow is snowy when it's snowing
I'm sorry it's slushy when it's going.

Ogden Nash

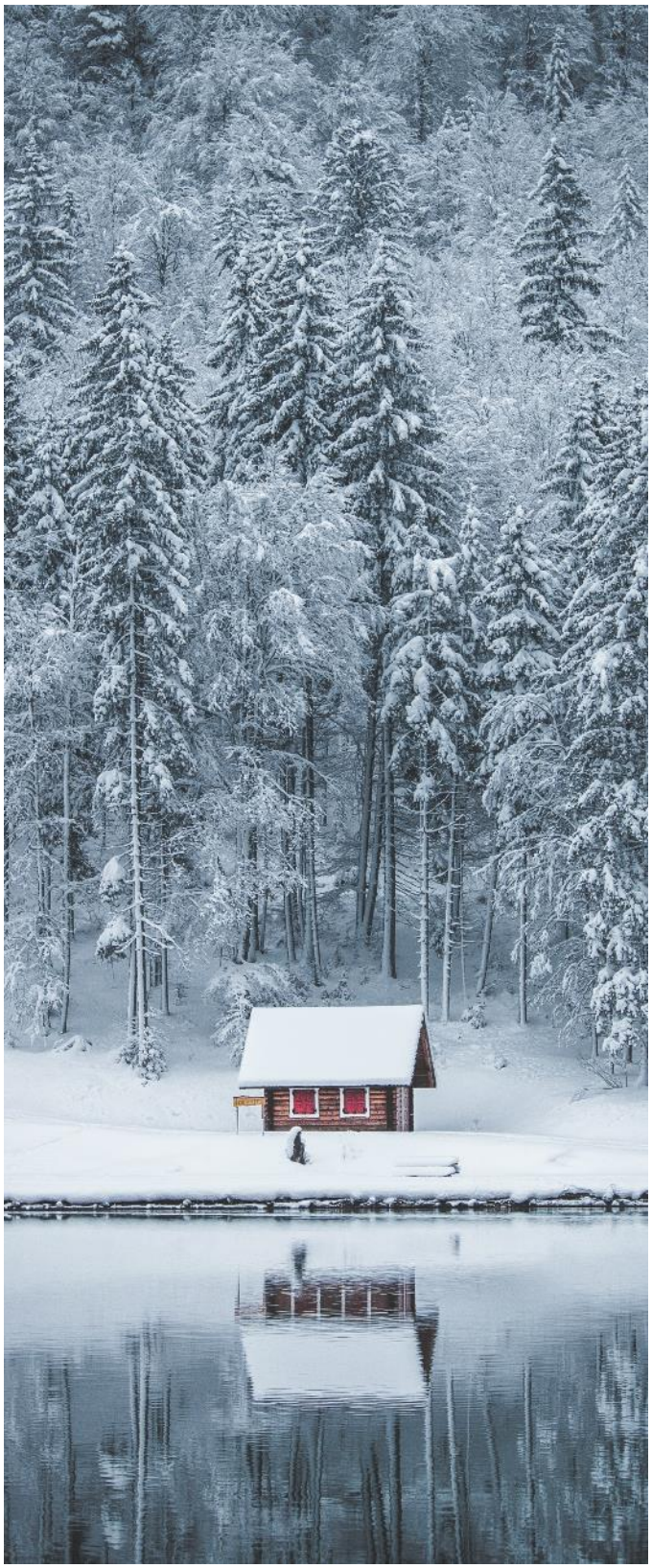
PFAS Regulations Adopted by the Washington Board of Health

The Board of Health's new PFAS regulations take effect on January 1, 2022. This regulation follows 2020 proposed legislation and 2021 Department of Health (DOH) PFAS rule making. Under these new regulations, State Action Levels (SALs) are established for five PFAS compounds and authorization is provided to DOH to develop maximum contamination levels if merited. PFAS SALs are established at the level where no known health effect has been identified for all individuals including at-risk populations. Water utilities are required to complete PFAS monitoring on a schedule determined by DOH, but no later than 2025. Waivers may be available from the DOH based on the utility's PFAS monitoring history.

If PFAS compounds are found, the utility must: complete confirmation sampling; increase monitoring based on the percentage of the SAL for the compound; investigate the possible sources of contamination; take action as directed by DOH; and importantly, provide public notification of the PFAS levels detected and actions taken by the utility.

While previous PFAS sampling identified a limited number of utilities in the state with positive PFAS results, advances in laboratory procedures now allow detections at much lower concentrations. Utilities must be aware that the potential for positive detections will be much higher under these new standards. If found, utilities may need to install treatment systems to remove PFAS compounds.

Finally, these new standards will allow the Department of Ecology to establish clean-up standards for the remediation of the contamination. Utility sources that require treatment may seek to recover treatment system costs from entities identified as having caused the PFAS contamination. However, at least initially, the utility will have to bear the costs of treatment, which reflects the utility's commitment to protecting public health and the supply of safe drinking water to the public.



Happy Holidays!