



The Tap



INSIDE THIS ISSUE:

AWWA Recommendations	3
Cyber-Security Attack	5
DOH Award	9

City of Bonney Lake

City of Fife

City of Milton

City of Pacific

City of Puyallup

City of Roy

City of Sumner

Covington Water

Firgrove Mutual Water Co.

Fox Island Mutual Water Association

Fruitland Mutual Water Co.

Graham Hill Mutual Water Co.

Lake Josephine Riviera

Lakewood Water District

Mt. View-Edgewood Water Co.

Parkland Light and Water

Peninsula Light Co.

Pierce County Planning & Public Works

PUD No. 1 of Thurston County

Spanaway Water Co.

Summit Water & Supply Co.

Tacoma Water

Town of Steilacoom

Valley Water District

Washington Water Service Co.

It Was a Dark and Stormy Night....

This is the way all great stories start, right? Well, those of you that have dedicated your lives to providing safe and reliable public drinking water probably know these words have a different meaning in your life. You understand all the elements (both natural and man-made... not to mention global pandemics!) that can come at you unexpectedly on any given stormy night or day. I understand firsthand what it is like to have the on-call phone ringing in the middle of the night and not knowing what awaits my husband when he heads out to respond to that call, often into inclement weather conditions. That is the story of providing safe and reliable public drink-

water. The one you and your staff live every day and night.

Over the years the Regional Water Cooperative of Pierce County (RWPC) has played a crucial role in providing safe and reliable drinking water to the over 800,000 residents of Pierce County (and many other counties as well). Your membership has also provided great support to Pierce County in helping to avoid receiverships—until that one dark and stormy night when the previously avoidable became unavoidable. Since 2012, Pierce County has been contacted by Washington Department of Health staff about five potential

failing water systems that were tipping into Receivership. In Washington State, the county where the failing water system is located ends up being the receiver of last resort. DOH requests the Superior Court to order the county take over the system in receivership. Through collaboration with and support of RWPC members, Pierce County and DOH were able to avoid receivership on four of these five water systems. Two of these systems were directly taken by Lakewood Water District and Thurston PUD and one received substantial support from Valley Water District. In November 2017, Kapowsin Water District became the unavoidable receivership, the one system that surpassed the ability of the membership to take on.

Even after drilling a groundwater well that didn't produce sufficient water to replace the spring source, Pierce County continues to pursue options to enhance this water system.

bhc
CONSULTANTS

- Water System Design
- Water System Planning
- Hydraulic Modeling
- RRA/ERP
- Electrical Engineering
- Structural Engineering

SEATTLE
TACOMA
BELLINGHAM

www.bhcconsultants.com

It Was a Dark and Stormy Night....

CONTINUED FROM PAGE 1

We expect these efforts will ultimately lead to a happy ending to this story. With continued support from RWPC members, whether by a phone call... "hey let me bounce this off of you", or "would you consider this?" ... or direct maintenance and operations for the Kapowsin water system, RWPC members are always willing and able to step in and offer assistance, support and expertise.

It has been my pleasure to work with such dedicated, knowledgeable and compassionate individuals over these years. I'm honored to have been elected to a board position with the RWPC and to work collaboratively with this membership over the years to find solutions for

happy ending stories. I will miss your special group very much as I move on to a new chapter in my life. My last working day with Pierce County is Thursday, 7/1/2021.

Kat Brooks,

Pierce County Planning & Public Works

Sewer Division Planning Manager



Brett Wise

Owen Equipment Sales **Website:** [Owen Equipment](#)

Phone: (253) 852-5819 **Cell:** (253) 249-6369

Address: 8721 S. 218th St Kent, WA 98033

Email: bwise@owenequipment.com

RWCPC Committees

Communications/Social Committee

Chair: [Christie Butler](#)

Vice-Chair: [Burt Clothier](#)

Emergency Management Committee

Chair: [Dan Sleeth](#)

Equipment/Resource Sharing Committee

Chair: [Chris Apple](#)

Executive Committee

Chair: [Larry Jones](#)

Legislative Committee

Chair: [Jeff Johnson](#)

Technical Committee

Chair: [Ben Lee](#)

Water Quality Committee

Chair: [Craig Downs](#)

Kennedy/Jenks Consultants

- Enduring relationships
- Trusted expertise
- Promises delivered

Over 120 Professionals in Washington & Oregon

◆ Asset Management and Master Planning	Seattle, WA (206) 652-4905
◆ Water Quality and Treatment	Federal Way, WA (253) 874-0555
◆ Source Development	Portland, OR (503) 295-4911
◆ Water Reuse	Eugene, OR (541) 338-8135
◆ Distribution and Pumping	
◆ Stormwater	

Visit our web site: www.KennedyJenks.com

- From: AWWA Public Affairs
- Date sent: 02/10/2021 07:02:21 am
- Subject: AWWA Security Advisory - Recommendations following Florida cyberattack

[Print This](#)

- Having trouble viewing the email below? Please [click here](#).
- Note: To ensure delivery to your inbox please add publicaffairs@awwa.org to your address book.



ALERT!
TO UTILITY MEMBERS

- Who: FBI, DHS, US Secret Service, Pinellas County Sheriff's Office
- What: Recommendations following Florida cyberattack
- When: Issued last night
- The Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), US Secret Service, and the Pinellas County Sheriff's Office have issued a [joint situational report](#) that concerns the water sector. EPA recommends that all water systems implement the mitigation measures listed at the end of this report where applicable.

Background

- On Feb. 5, 2021, unidentified cyber actors obtained unauthorized access, on two separate occasions, approximately five hours apart, to the supervisory control and data acquisition (SCADA) system used at a local municipality's water treatment plant. The unidentified actors accessed the SCADA system's software and altered the amount of sodium hydroxide, a caustic chemical, used as part of the water treatment process. Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change. As a result, the water treatment process remained unaffected and continued to operate as normal.
- The unidentified actors accessed the water treatment plant's SCADA controls via remote access software, TeamViewer, which was installed on one of several computers the water treatment plant personnel used to conduct system status checks and to respond to alarms or any other issues that arose during the water treatment process. All computers used by water plant personnel were connected to the SCADA system and used the 32-bit version of the Windows 7 operating system. Further, all computers shared the same password for remote access and appeared to be connected directly to the Internet without any type of firewall protection installed.

Recommended Mitigation

- Restrict all remote connections to SCADA systems, specifically those that allow physical control and manipulation of devices within

the SCADA network. One-way unidirectional monitoring devices are recommended to monitor SCADA systems remotely.

- Install a firewall software/hardware appliance with logging and ensure it is turned on. The firewall should be secluded and not permitted to communicate with unauthorized sources.
- Keep computers, devices, and applications, including
- SCADA/industrial control systems (ICS) software, patched and up-to-date.
- Use two-factor authentication with strong passwords.
- Only use secure networks and consider installing a virtual private network (VPN).
- Implement an update and patch management cycle. Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected systems for known vulnerabilities and software processing Internet data, such as Web browsers, browser plugins, and document readers.

AWWA's resources for [cybersecurity](#) provide guidance on best practices and training opportunities to help water systems actively engage and implement a cybersecurity risk management strategy, including resources specifically developed to support [small systems](#):

- [Water Sector Cybersecurity Risk Management Guidance and Assessment Tool](#)
- [Cybersecurity Risk & Responsibility in the Water Sector](#)
- [Cybersecurity in the Water Sector eLearning Course](#)
- [USDA Small Systems Instructor-Led Cybersecurity Course](#)

In addition, the [WaterISAC](#) is another resource that utilities can use to monitor threat information. Most resources require membership, but utilities can get access to the restricted items associated with the [incident in Florida](#) by signing up for a free two-month trial.

Questions can be directed to [Kevin Morley](#), federal relations manager.

PACIFIC groundwater GROUP
Water Resource & Environmental Consulting

Water Resources

- Groundwater Development and Planning
- Water Rights Permitting Support
- Modeling Groundwater Flow Systems
- Saltwater Intrusion Evaluations

Land Use/Development

- Stormwater Management
- Hydrologic Effects of Land Development
- Property Transactions & Site Assessments

Environmental

- Remedial Investigations/Feasibility Studies & Cleanup of Upland and Sediment Sites
- Landfill Monitoring/Permitting
- Cost Allocation

www.pgwg.com

2377 Eastlake Ave E. | Seattle, WA | 206-329-0141
2417 Pacific Ave SE. | Olympia, WA | 360-413-1510

Cyber-Security Attack on Florida Water System

Reviewing the Oldsmar Florida Cyber Security Breach

Looking at the AWWA Security Alert above, let us review the known issues that either contributed to the breach, or were identified as a potential risk during the investigation and why the issue created a cyber risk or liability for the municipality:

“Remote access to the SCADA system was obtained through a commonly used remote access software tool, TeamViewer. The TeamViewer client employed a simple password, allowing the cyber actors to gain access.”

Using TeamViewer for remote access. I would classify TeamViewer and a step above free remote access software such as VNC. It is not a business class solution. TeamViewer is free for non-commercial use and can easily be obtained by anyone with access to the internet. TeamViewer employs a direct connection model. What this means is that the remote client can connect to any TeamViewer client and take control if the password is known, exposed, or cracked.

TeamViewer does not enforce use of a gateway to verify the identity of remote access users prior to connecting to the TeamViewer host. If you are currently using TeamViewer, VNC or some other free or inexpensive remote access solution, consider changing to a system that requires secure, verified multi-factor authentication prior to accessing the remote resource.

Employing simple passwords. Using a simple password is just inviting someone to compromise your protected resource. Cyber criminals look for simple passwords all the time. Why? Because they are easy to guess with very little effort. Using “Password” or “Welcome” as your password is asking for trouble.

“The municipality had several computers running TeamViewer for remote access, and all the TeamViewer clients used the same simple password.”

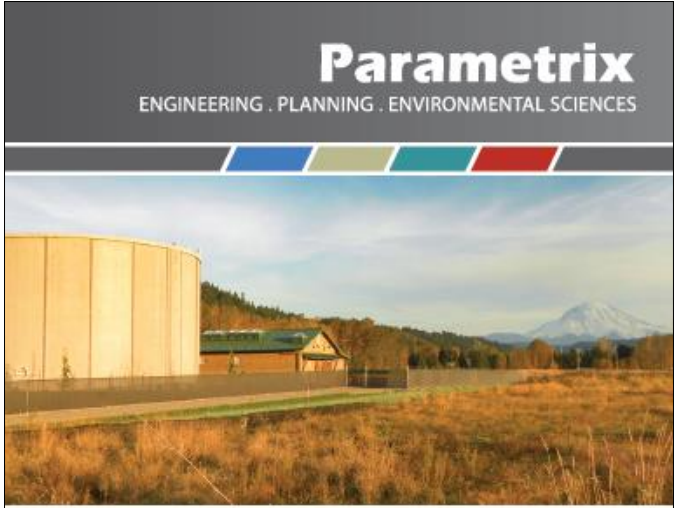
Using the same password to protect multiple

resources. Using the same password for all your potential points of entry provides easy access to protected resources if this password is ever compromised. If this is your current practice, consider changing your password policies as soon as possible.

“Additionally, it was noted that there was no firewall protection installed for these TeamViewer clients and all the computers in use at the treatment plant were attached to the SCADA system and running 32bit versions of the now out of support

Windows 7 Operating System.”

No firewall? No excuse. Not protecting your technology resources and assets with a properly configured, business class, frequently tested and maintained firewall is inexcusable. The firewall exists to protect your resources, it allows specific, designated traffic to traverse between your intranet and the public internet. Ideally this network should have been protected with a firewall meeting the aforementioned criteria and any access through the firewall should have employed the use of an



Parametrix
ENGINEERING · PLANNING · ENVIRONMENTAL SCIENCES

Helping clients with water resource management, water systems, and drinking water quality since 1969

Cyber-Security Attack on Florida Water System

Reviewing the Oldsmar Florida Cyber Security Breach

CONTINUED FROM PAGE 5

encrypted VPN connection.

Sharing a Network with SCADA. The municipality failed to isolate its SCADA system from the on-premises network. Any breach of the on-premises network provided access to the SCADA network as well. Isolating SCADA from the production network affords additional protection and controls on who can access SCADA.

Still using Windows 7. Windows 7 is out of support. You can longer obtain support from Microsoft and they are no longer issuing patches

and fixes to correct vulnerabilities. This creates a problem because hackers still look for and identify vulnerabilities and exploits in Windows 7. Using these exploits and vulnerabilities; cyber criminals can scan for, find and gain access to computers running Windows 7 or older with relative ease. Many older SCADA systems may require a specific version of Windows to run SCADA client software and will not run on Windows 10. If you are facing this challenge, contact your vendor to find out what steps are needed to bring

your PC's and servers up to date.

How do I protect my Technology Assets and Resources?

- Firewall**
 Protect your network with a business class firewall. If you are currently using a residential class firewall replace it as soon as possible. The firewall should sit between your internet gateway and your network. Your business class firewall will include a detailed logging feature. Turn it on and keep your logs for at least 2 years. Ensure any updates from the firewall manufacturer are loaded in a timely manner. Perform penetration tests on your firewall monthly, and any time a change is made to the firewall or if an update has been loaded. Ensure any traffic entering your network from the public internet is using an encrypted connection or better yet, a VPN.
- Multi-Factor Authentication (MFA)**
 Multi-Factor authentication adds a second authentication method in addition to a password, usually a text message with a verification code. Most users are already familiar to this concept as most banks and financial institutions use this method of authentication. Adding multifactor authentication adds a nearly foolproof level of security to your identity verification. This should be enabled for all users accessing
- SCADA**
 Isolate your SCADA system from your production network. They should sit on

different physical networks. If you need to route traffic from your production network to your SCADA network employ a second firewall and VPN between the two networks. User access to SCADA should be restricted to only those who need access. If you are using the public internet to communicate with remote sites ensure you are using a secure VPN and protect your remote site with a business class firewall as well.



Cyber-Security Attack

Reviewing the Oldsmar Security Breach

CONTINUED FROM PAGE 6

Your entity's resources, especially for accessing critical resources such as SCADA or financial records. Enabling MFA can be complicated and should not be undertaken without a clear understanding of the process. Misconfiguration can effectively bar your users from the ability to log into resources. Consult with your IT provider before enabling this feature on your resources.

- **Remote Access Solution**

A big subject for short article. If you allow remote access to your resources, it is critical that it is configured in a secure manner. Remote Desktop, VNC and TeamViewer should only be used if the connection is made over a VPN. If you are using one of these solutions and not utilizing a VPN you are asking for trouble. If your entity is using



CHS ENGINEERS

- District Engineer
- Design
- Modeling
- Special Studies
- Comprehensive Planning
- Construction Management

JULIE'S

- Reservoirs
- Pump Stations
- Treatment & Reuse
- GIS-Surveying & Mapping

www.chsengineers.com
12507 Bel-Red Road, Suite 101, Bellevue, WA 98005
425-637-3693

Remote Desktop, consider changing the default port from 3389, as it is one of the most scanned and attacked ports on the internet. A better solution is to use a gateway, that multi-factor authenticates your users before the connection is made, and the gateway brokers the connection to the remote resource, the remote user never connects directly to the remote resource. Solutions from LogmeIn and BeyondTrust meet these requirements.

- **Frequent Tested Backup**

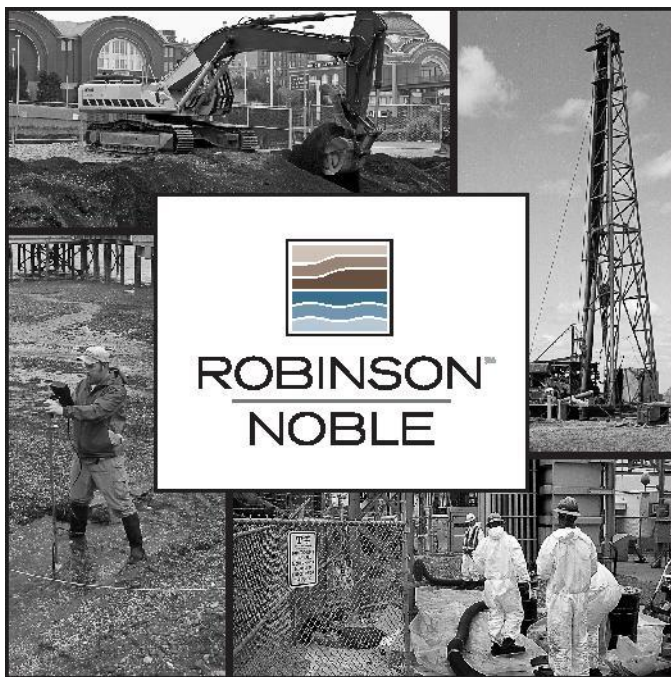
Your last and most important line of defense is your daily backup. In the event of a Ransomware event it could be your only chance of avoiding a very costly ransom. If you are still backing up to tapes, consider switching to a disk-based backup instead. Tapes fail. Disk based backup is faster for both the backup and the restore process, and

more reliable than tape. Keep at least a weekly backup offsite. If you store the tapes offsite.

If you are using disk-based backup subscribe to a cloud service, if you do not already have one, and copy the backups to the cloud during off hours. Whether you are using tape or disk-based backup, it is critical that you test your backups by performing a test restore at regular planned intervals. Testing allows your IT staff to be familiar with the process in the event of a critical situation and verifies the validity of your backups in advance of needing them.

- **Update your Systems**

Keep your systems up to date. Software vendors frequently issue patches to correct both flaws in their products and identified security issues. Implement a verifiable patching and update program to keep your



ROBINSON NOBLE

Supporting water purveyors for over 70 years

Groundwater Development, Monitoring & Protection • Regulatory Compliance & Permitting • Emergency Response Services • Geotechnical Engineering • Site Investigation & Remediation

Tacoma
252.475.7711

www.robison-noble.com

Woodinville
425.488.0599

Cyber-Security Attack

Reviewing the Oldsmar Security Breach

CONTINUED FROM PAGE 7

- systems up to date.

These are just a few of the controls for maintaining an effective Cyber-Security program. An effective Cyber-Security program touches on much more than the items briefly touched on in this article. It requires commitment from leadership, both in the commitment of resources and commitment to enforcement of Cyber-

Security policies in your organization. It requires knowledgeable IT resources who can implement and test solutions as well as education for your workforce; particularly your less technical staff as some policies may add a level of complexity they are not accustomed to.

Christian Fast,
Lakewood Water District

Check out the new Grant/Loan Opportunities page on our [website](#).

Thanks to our Technical Committee for compiling this information. Please share any grant or loan programs you know of that are not on this list. We will be working to keep this information as current as possible.

For questions or suggestions for this list, please contact our Technical Committee Chairperson, Ben Lee:
BLee@landauinc.com

Regional Water Cooperative of Pierce County
PO Box 11359
Tacoma, WA 98411

Upcoming Meetings

RWCPC Monthly Meeting – Thursday, August 12, 2021, 9:00 a.m.

Host: Washington Water, virtual meeting

RWCPC Monthly Meeting – Thursday, September 9, 2021, Noon

Annual BBQ Meeting

Host: Town of Steilacoom – 2701 Chambers Creek Road, Steilacoom, WA

RWCPC Monthly Meeting – Thursday, October 14, 2021, 9:00 a.m.

Host: Mt. View-Edgewood Water – virtual meeting

RWCPC Monthly Meeting – Thursday, November 11, 2021, 9:00 a.m.

Host: City of Puyallup – 1100 39th Ave SE, Puyallup, WA

RWCPC Annual Meeting & Dinner – Thursday, December 9, 2021, 6:00 p.m. (9:00 a.m. if meeting is virtual)

Host: Pierce Co. Planning & Public Works – Pierce County Environmental Services Building, 9850 64th St W, University Place, WA

RWCPC Wins Commitment to Excellence Award

Washington Department of Health Recognizes Co-op Efforts



The Regional Water Cooperative was awarded the Commitment to Excellence Award by the Department of Health during this year's Drinking Water Week, May 2 to May 8.

An award ceremony was held at Firgrove Mutual on May 24 for DOH staff to present the award to the Co-op. Members and special guests Marc Marcantonio and Mike Ireland were in attendance.



President Larry Jones shows off the Commitment to Excellence Award



DOH published the following notice of the event: **Regional Water Cooperative of Pierce County (RWPCPC)**. RWPCPC led the way when it established a monthly networking and knowledge-sharing forum in 1991, which has grown over the years. Through collaboration and diligence, RWPCPC addresses challenges to local utilities through the forum including water quality, legislation, emergency preparedness, and more. They are a unique action-oriented organization, dedicated to helping and sharing the best management practices. Pierce County residents enjoy better drinking water due to the work of the RWPCPC.