

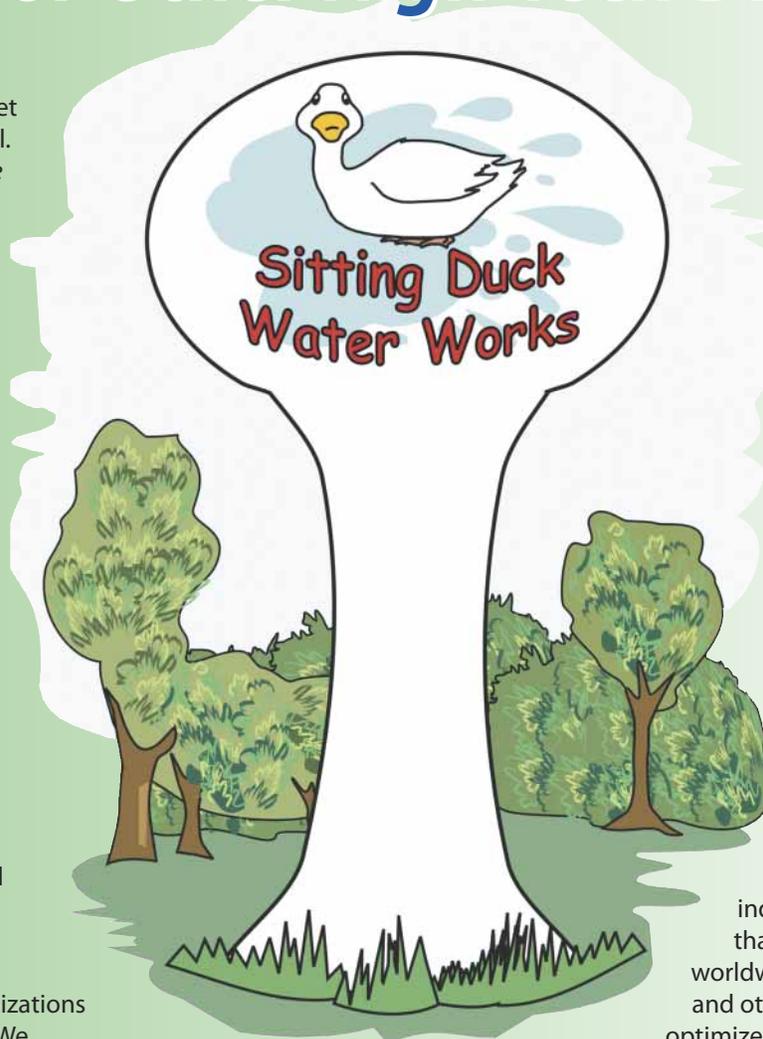
Computer Corner

Don't Be a Sitting Duck for Cyber Attacks or Other High-Tech Disasters

America has received yet another “wake-up” call. On May 8th, 2021, *The Washington Post* reported: “Ransomware attack leads to shutdown of major U.S. pipeline system.” Luckily installation of a new Automated Supervisory Control and Data Acquisition (SCADA) Industrial Control System (ICS), allowing remote control, had not yet been fully completed or the disaster would have been even greater. A portion of the Colonial pipeline remained operational only because it could still be manually controlled.

Eric Goldstein, Executive Assistant Director of the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) stated, “This underscores the threat that ransomware poses to organizations regardless of size or sector. We encourage every organization to take action to strengthen their cybersecurity posture to reduce their exposure to these types of threats.”

Small towns, large cities and rural water districts need to heed Goldstein’s words – “regardless of size.” A recent case-in-point is a cyberattack that took place just this year. In February 2021, the water treatment plant of Oldsmar,



Florida allowed an attacker to remotely access the water system controls and add dangerous amounts of chemicals to the town's water supply through a commonly used remote access software program.

The water system’s employees routinely accessed control systems using mobile phones, tablets or remote computers. The hacker gained remote access through TeamViewer software, widely used in the water industry and on more than 2.5 billion devices worldwide. While this program and others like it offer ways to optimize security, often the agencies using it do not employ those

protections finding it to be more convenient to go without them. That is only one of the security elements that should be considered.

The cyberattacker changed the levels of liquid sodium hydroxide to more than 100 times the normal dosage. Sodium Hydroxide is the main ingredient in drain cleaners.

Many water systems in Kansas use small amounts of liquid sodium hydroxide to raise the pH level of the water. Had an employee not happened to look up at his computer screen at just the right time to notice the cursor moving, not by his hand, this incident could have had tragic results.

Austin Berglas, the former head of FBI NY Cyber stated, "Water facilities rely on SCADA systems to manage the automated process of water distribution and treatment. Many of these industrial control systems are outdated, unpatched, and available for review on the Internet, leaving them incredibly vulnerable to compromise."

"In addition, many ICS solutions were designed for non-Internet facing environments and therefore did not incorporate certain basic security controls. This offers additional vulnerabilities as more and more operational technology environments are allowing access to their ICS systems from the Internet," Berglas added, 'highlighting the vulnerability of certain critical infrastructure when their ICS systems are allowed to be exposed to the Internet and not isolated.'

The Covid-19 pandemic has resulted in many water utilities using remote access tools like TeamViewer and increasing numbers of systems choosing to automate with SCADA and ICS solutions. But, increased automation and remote access makes it increasingly easy for even average hackers to find and hit unprotected targets and do damage.



Important questions for water and wastewater utility personnel . . .

The important questions all operators, managers, board and council people should be asking themselves is if they have become overly reliant on technology?

- Can our facilities continue to function if technology fails?
- If a SCADA system were to be attacked, shutdown, or fail, can it continue to safely operate?
- Is a water system Internet dependent or can it function without the worldwide web?
- Is the treatment plant, delivery system, backup system or office computerized system remotely accessible or Internet dependent?
- If hacked or attacked, would the water system come to a screeching halt?
- Is there a danger of manipulation of chemical levels and other potentially dangerous functions up to and including financial exposure?
- Is the system kept up-to-date with all the latest security patches and updates?

It is HIGHLY recommended that all remote devices used in water utilities use "second factor user authentication" (a CODE is sent to the authorized mobile/remote device that must be entered to verify user identity). Yes, people complain that it is a nuisance, but it is an important safety precaution. Water system remote access should also have rules to prevent password-reuse, and not allow acceptance of commonly used weak passwords like "1234" or "password." Any remote access solution should also have a "Lockout" policy if multiple incorrect passwords are entered. Hacker programs can attempt thousands of possible password combinations in seconds. They can recognize all your tricks like "fo0+Ba1l" (football) and "S0ck3+" (socket). Hackers will even investigate a water systems employee's social media for names of pets, grandchildren, etc, in order to break-in.

Cybersecurity experts increasingly fear attacks on water utilities as more water systems, dams, and pipelines install computerized systems that allow monitoring of water and chemical levels from remote and mobile devices.

Pat McCool who is a consultant on KRWA staff, says: "A Kansas water plant was recently shut down by cyberattack." The best thing about SCADA systems is you can remotely monitor your plant status and make immediate decisions about how to react to a small or large problem." Pat advises against being able to alter chemical

dosages remotely. Pat also says, "Being able to remotely receive notification alarms of a problem and then being able to determine the severity of the problem are real assets to monitoring plant operations; for example, shutting down the plant if the water treatment process is compromised." Pat also stated that it's nice for the operators to at least be able to shut off a problem piece of equipment or plant in the middle of the night and fix it a few hours later. He also advises that to ensure everything is working correctly, manual, routine monitoring must also take place.

Technology is a wonderful thing. But, as decision-makers for a utility system, the convenience and advantages of implementing the latest new technological innovation must always be weighed against the cost, disadvantages and risks. Decision-makers should be informed and wise to best serve and protect their community. And, if a new technology is installed, security protocols must be followed. There's nothing wrong with being able to fall back on the old fashion way of performing a task when needed.

Many have had the experience of being told by a store clerk or the kid at the drive-thru window that they can't make change for them until their IT person fixes the computer. That is tech dependency run-a-muck!

Technology sometimes lets us down. Recently I received a call from a Missouri water system that had performed a task repeated thousands of times across each month. They had loaded up their new laptop and electronic read equipment into the truck to "radio read" meters. Twenty

It appears the problem resulted from the new laptop using more than double the wattage of their old laptop, at 230 watts. And, the combined electrical current draw of laptop and radio read equipment exceeded the capacity of the circuit. The result was an inoperable computer and truck!

minutes later, the laptop is dead, the truck has multiple fuses blown and the new computer-controlled truck transmission is stuck in reverse and will not shift gears. What a disaster! It appears the problem resulted from the new laptop using more than double the wattage of their old laptop, at 230 watts. And, the combined electrical current draw of laptop and radio read equipment exceeded the capacity of the circuit. The result was an inoperable computer and truck!

When it works, technology is wonderful, when it doesn't, well . . . It is important to have backup plans in place. Remember Murphy's Law: "Anything that can go wrong will go wrong." Be Wise – Be Safe!

Merle Windler and his wife Linda are owners of Thoroughbred Systems, Topeka. The company specializes in software solutions for utilities and municipalities, computer networking and associated training. Contact: merlewindler@yahoo.com



DHS - CISA Offers Security Assessments to Water and Wastewater Systems

Did you know that the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA) has two consultants assigned to the state of Kansas that are available to conduct FREE physical and cybersecurity assessments for water and wastewater systems? These assessments help systems identify safety issues and vulnerabilities to a wide variety of potential hazards. These assessments are completely voluntary and non-regulatory – meaning, if any issue is identified during the assessment, there is no obligation to the system to correct the issue. If you are interested in participating in a security assessment, contact one of the following consultants:

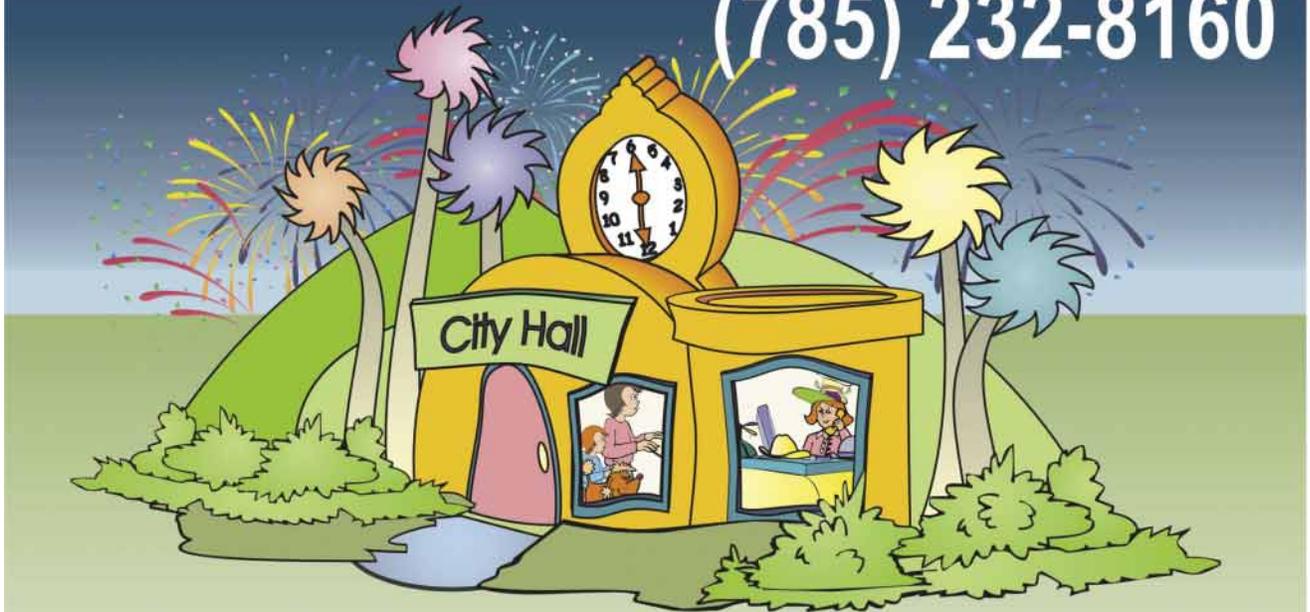
Chuck Clanahan, CPP

Protective Security Advisor – Kansas District
U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
(785) 213-8699, chuck.clanahan@cisa.dhs.gov

Geoff Jenista, CISSP

Cybersecurity Advisor, Region VII
U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
(913) 249-1539, Geoffrey.Jenista@cisa.dhs.gov

Thoroughbred Systems 116 SE Ave Topeka, KS 66603-3905
(785) 232-8160



Our Success Is Measured By How Well You Succeed!

Our customers are known to wear many hats,
Billing, court docket, even licensing cats.
So we listen quite closely when you say what you need,
For our success is measured by how well you succeed.
Whether it's billing for water or sewer or trash,
Tracking the charges and banking the cash,
For the town cemetery, Knowing who's in what plot,
Tbred's got software that can help you... a lot!
And people to help with your financial woes,
Folks that know just where each decimal goes.
Utility programs that handle gas... electric too,
Touch read, radio read, and Satellite... Newer than new,
We can email your statements and do Internet pay,
Automatic banking, for us, it's child's play.
So call and visit with us, for a minute of two,
For we'd love to show you, what's newer than new!

To the people of water boards and city councils and staff, across this land, from clerks to operators to police to dispatchers & more, who work to keep our water & our streets safe every day, Happy 4th of July USA Independence Day & thank you for your service.