By Elizabeth Dietzman, JD

How to Live With CyberINsecurity

Even small water systems are going to get hacked. In February 2021, in Pinellas County Florida, hackers gained access to the water facility control systems for the 15,000-person town of Oldsmar, and tried to raise the sodium hydroxide content in the water supply. Obviously, in high enough concentrations this could be deadly, but early detection by an alert employee stopped the incident from becoming more serious. Turns out that the treatment plant had used multiple computers running an older version of Microsoft Windows to monitor the facility remotely and all of the computers shared a single password.

Before that, in March 2019, the Post Rock Water District in Ellsworth, Kansas, which serves around 1500 residential and ten wholesale customers, was hacked. The hacker was a disgruntled former employee who remotely accessed one of Post Rock's Water District computers to shut down the cleaning and disinfecting procedures. During his employment, the employee had accessed a computer remotely after hours in order to monitor the plant. However, his credentials were not revoked after he resigned, so he still had access. And a grudge, apparently.

Are water systems, large and small, at risk from cyber attacks? Yes. This is no secret. That's why there are requirements at the federal level that are designed to address this. On October 23, 2018, America's Water Infrastructure Act (AWIA) was signed into law. AWIA Section 2013 requires community (drinking) water systems serving more than 3,300 people to develop or update risk assessments and emergency response plans (ERPs). By now all systems that qualify are required to have an ERP in place. The ERP shall include:

1. Strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system
2. Plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water
3. Actions, procedures and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes and construction of flood protection barriers; and
4. Strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.

Let's be clear – "malevolent act" in this day and age pretty much means an attack by a hacker or a terrorist. And it is much easier to disrupt a water system using a keyboard than explosives.

Are water systems, large and small, at risk from cyber attacks? Yes. This is no secret.

There are also nationally adopted cybersecurity standards like the NIST Cybersecurity Framework. Here is a quote from the www.nist.gov website: “The Framework not only helps organizations understand their cybersecurity risks (threats, vulnerabilities and impacts), but how to reduce these risks with customized measures. The Framework also helps them respond to and recover from cybersecurity incidents, prompting them to analyze root causes and consider how they can make improvements. Companies from around the world have embraced the use of the Framework, including JP Morgan Chase, Microsoft, Boeing, Intel, Bank of England, Nippon Telegraph and Telephone Corporation, and the Ontario Energy Board.”

So we are aware that cyber attacks can happen and some really smart folks have addressed this. Except that I don’t know many small water systems that can implement cybersecurity at the level of Boeing and Microsoft. The problem is that small systems are already struggling to make ends meet and it simply isn’t realistic to take all the steps that cyber security experts would recommend. Especially knowing that even if you do every single thing you possibly can, you can always still be hacked.

THAT is the dirty little secret about cybersecurity that no one really mentions: there is no way to guarantee that you won’t be hacked. There is no absolute cybersecurity. There is only cyberINsecurity! Yes, I said it. No matter what steps you take, no matter how much money you spend, if you are connected to the Internet, and someone wants use your computer to gain access to your system badly enough, they will. When even the United States Government has been hacked and has had really sensitive data compromised, what chance does a small water or sewer system have against hackers? NONE. Instead, small systems need to focus on a sensible two-step risk-benefit analysis approach that explores what they can afford. Think Lemonade and Chickens!

1. You have to decide how much cyberINsecurity you can live with. I call this the Lemonade Analysis – is the juice worth the squeeze? You balance limiting the risk against take the steps that you can afford to take.
2. Knowing that no matter what you do, you can always be hacked, you need a plan for recovery – also known as COOP – a Continuity of Operations Plan. After you are hacked, what will you do in order to keep providing safe drinking water?

THAT is the dirty little secret about cybersecurity that no one really mentions: there is no way to guarantee that you won’t be hacked. There is no absolute cybersecurity. There is only cyberINsecurity!

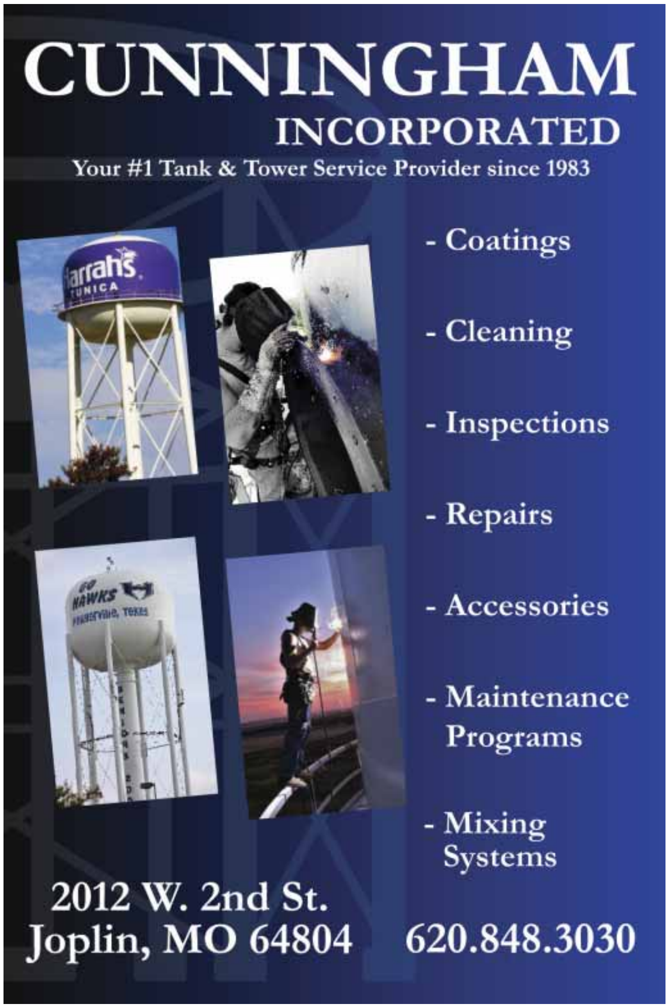
Lemonade

One of the first things to think about when it comes to cyberINsecurity for a small system, is the fact that you can make a calculated guess about who might want to hack into your system. A good analogy overall is to think about fire protection. Yes it is true that a forest fire could destroy your house or a gas main could blow up and set your neighborhood on fire. So you could build a huge underground bunker for your house and have fire towers set up with infrared scanners. And you could install a huge fire suppression system around your property. But unless you live in California or Australia, where sadly forest fires have become a way of life, it is much more statistically likely that faulty wiring, a stove-top burner left on or a candle would cause a fire first. So making sure that you have working smoke detectors and no frayed lamp cords and good fuses is a much less expensive solution to a much more likely problem.

CyberINsecurity can be analyzed in a similar way. Hacking occurs when someone who is not authorized takes steps to gain access to your computer and through it, the information it contains (the data.) This is usually done by tricking a user into giving out their password, because the password is the key that unlocks access to the system. Overall, cybersecurity is an endless game of cat and mouse between bad guys (the cat) aka the people who want access to your system – and you (the mouse.) (Don't forget! Who usually wins the game of cat and mouse in the end? The cat!) Once the hacker gets access to a computer, they can sell those credentials to other bad guys or use them directly to steal data, cause problems, etc.

Hackers also come in different flavors, which can help you with your cyberINsecurity analysis. There are nation states hackers who work for the countries who are attacking one another. Russia and China and others have entire groups of hackers whose sole job is try to penetrate our government systems. Then there are hackers who do it for fun and bragging rights. Then there are hackers who do it for vengeance, such as a disgruntled employee. There are also hackers who do it for money, i.e., making you pay to get your data back (aka ransomware) or selling your data to other parties.

Keeping in mind that a hacker will get access to your system if they really want to, you have to look at how much effort a hacker is likely to spend and how much you can afford to spend on defenses. There are all sorts of defenses but ultimately it all boils down to how much you can afford to spend as a small system. Is the juice worth the squeeze? Is it more likely that a small water system is going to be targeted by a disgruntled former employee or that a nation state is going to target your system? If you are the Metropolitan Water District (MWD) of Southern California, the largest supplier of treated water in the United States, a critical utility upon which 19 million people depend for their water, you are likely to be the subject of ongoing cyber attacks by nation states hackers and ransomware hackers. MWD owns and operates an extensive water system including the Colorado River Aqueduct, 16 hydroelectric facilities, nine reservoirs, 819 miles of large-scale pipes and five water treatment plants.

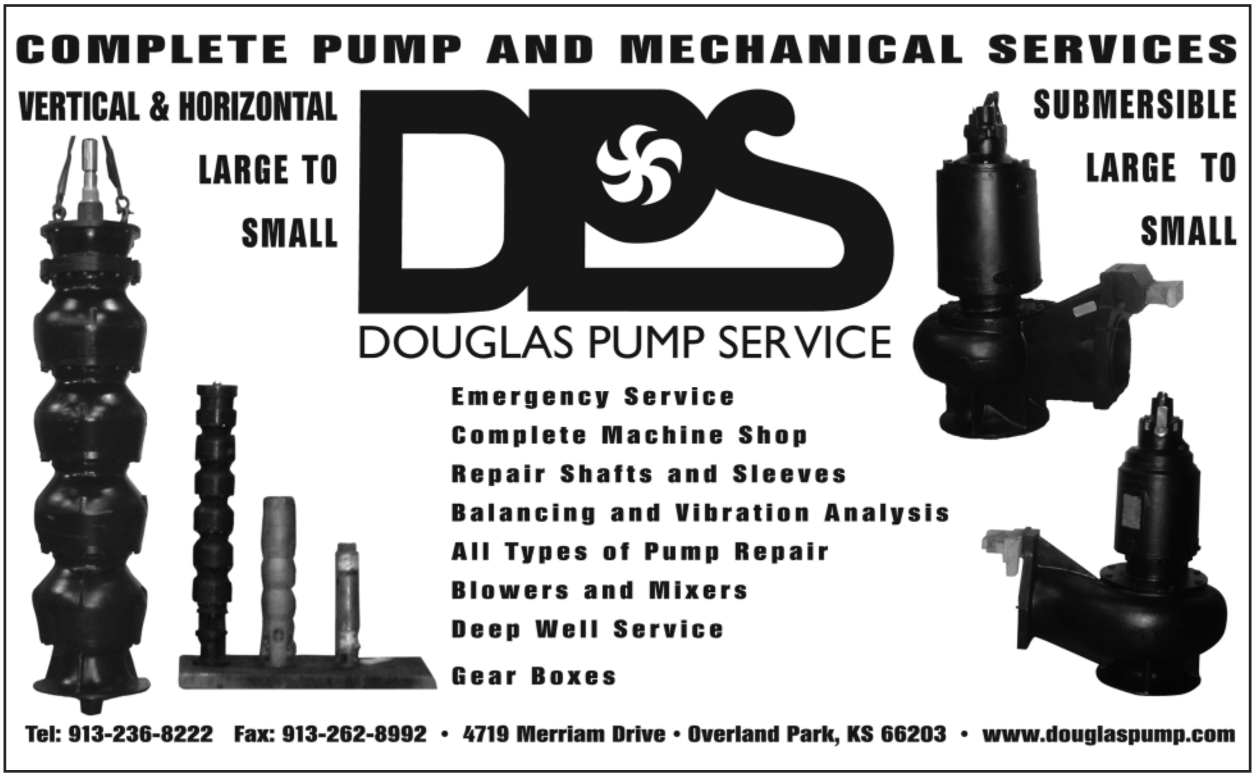


Four of these treatment plants are among the ten largest plants in the world. So it makes sense that they have spent millions and have implemented continuous threat monitoring, risk and vulnerability management, and asset management procedures for their vast operational technology/industrial control systems network. MWD is absolutely right to worry about being targeted by a bad nation state or a hacker who wants to charge them millions for their own data. However, if you are a small water system with a few thousand users, I would be more worried about a former employee or a casual hacker who wants to make a quick buck or just cause trouble.

I'm not going to explain all the things you need to do in order to maintain good cyber hygiene. Google "cybersecurity" and there are millions upon millions of articles telling you to upgrade your antivirus software, change passwords, update software versions, etc, etc. Training is everywhere. KRWA recently offered cybersecurity training. InfraGard, a national critical infrastructure program affiliated with the FBI is free to join. InfraGard offers "educational programs and information-sharing initiatives that truly adapt to the unique threat environments, critical infrastructure landscapes, and security needs of their specific regions, (www.infragard.org)". Contact infragardteam@infragard.org for membership information or InfraGard at InfragardHeadquarters@ic.fbi.gov

Google "cybersecurity" and there are millions upon millions of articles telling you to upgrade your antivirus software, change passwords, update software versions, etc, etc. Training is everywhere. KRWA recently offered cybersecurity training.

However, based on the most likely type of cyberattack on a small system, I will tell you that the two most important things that you can do to protect your system is to teach your employees to protect their passwords and practice cyber-psychology in order to avoid phishing attacks. In both the Florida and Post Rock cases, the "hacker" had passwords all but handed to them. I would argue that the Post Rock hacker wasn't even really a hacker. Just a former employee who used his same password! In both of these examples, very simple and inexpensive steps could and should have been taken to protect the systems: changing passwords! Change them every six months. Change them anytime an employee leaves. Set up that annoying two-step process, where you have to enter a separate code that you receive by text in addition to entering your password. The next most important thing you can do is tell your employees to watch out for phishing! Phishing is a type of trick aimed at computer users, often described as a social engineering attack. The goal is to fool the user into giving up



information, including login credentials. It occurs when an attacker, masquerading as a trusted entity, tricks a user into opening an email, instant message, or text message.

Verizon publishes a huge report every year called the Data Breach Investigations Report that analyzes data breaches. Ninety percent of data breaches in 2020 and the several prior years involve phishing. That email telling you that your bank account has been accessed and asking you to provide all your account info? A fake. That text from your boss asking for the password to the billing software? A fake. That email telling you that you won Superbowl tickets – just click here to redeem them – fake. The real problem is that employees are the weakest link in cybersecurity, because they are connected to the internet and can be fooled. So as long as you have employees who are connected to the internet, you can be hacked. Training your employees in cyber-psychology is an inexpensive way to protect your system.

But someday you might be hacked . . .

A stick drive for less than $50 would probably hold all your data too. Back up often! Back up in multiple ways!

Chickens

That is where the chickens come in! What will you do after you are hacked? How do you structure your COOP? Again, there are lots and lots of free and not so free plans, templates, and resources that you can use to create a COOP. The question is, how much can you afford to spend to create one and also to keep it updated? Ironically small systems have an advantage when it comes to continuity of operations, because many of them have been late to the dance on computer systems. That can cut in your favor! The average small system uses computers for billing and bookkeeping and may also have SCADA software that allows remote monitoring, especially after hours. So you have to protect your data and protect your system's operations. Your data is most vulnerable to what is called a ransomware attack.

After a hacker gets passwords, they can get control of your computers and encrypt the contents, making them unusable until a payment is made. After you pay, the hackers promise to give you a decryption key – a complex series of letters and numbers that will unlock your system. Often victims pay ransom because they have no backup copies of the infected systems or because the effort required to restore hundreds of computers is prohibitive. But as a small system, it is probably not impossible to keep hard copies of data like your customer lists and billing information. A stick drive for less than $50 would probably hold all your data too. Back up often! Back up in multiple ways! That will allow you to keep sending out bills and track budget info even if you are hacked or face some other kind of catastrophic failure. Keep in mind that if your system is hacked, you will need to hire someone to set up new software and you will need to re-enter your data from those clean backups. The reality is that I know really small systems that still walk and manually read their meters or have customers self-report usage and use simple billing software that isn't connected to the Internet. They aren't really going to be impacted by a hacker. So think back to the days before you used computers. How did you read meters, set up new accounts and do your billing? You may be able to use those techniques as part of your COOP.

The other thing you have to protect is your operating system. As you may recall from both Florida and Post Rock, the "hacker" was someone accessing the actual water system operations software and trying to change the way that the water was treated. In both cases, alert employees detected the intrusion. Just like employees can be the biggest weakness, they can also be the biggest defense. So you will definitely need to think through the exact mechanics of how you will detect an intrusion and how you will function manually. Now for small systems, this is doable. If you don't still have that guy who remembers how to manually check chemical levels and drive out to the well-house and check a flow meter, then consider training someone up to do this. Just imagine what it would take to operate the system if no computers existed. This would be almost impossible if you are the largest supplier of treated water in the United States, but very feasible if you have a handful of wells and simple operating systems.

Ask yourself how the folks who started the water systems handled operations? Because back in the 1950's, 60's and 70's when a lot of small water systems were formed, they definitely did not use SCADA systems. I have heard stories of board members who checked well-houses after power outages and bad storms and did water-sampling themselves. This type of hands on operating could be the solution. But if you don't have an operations employee who knows how to do all of this manually, then cross-training someone could be part of your COOP. You need to have a plan for COOP anyway. Depending on where your system is located or how robust your system is, you should always have a COOP. For treatment plants located along a river, flooding could be a much bigger danger than hackers. For systems in the West, forest fires have become a huge problem. Cybersecurity is just one of many reasons that a system can no longer provide drinking water and your COOP should address all of them.

Cybersecurity is just one of many reasons that a system can no longer provide drinking water and your COOP should address all of them.

Just remember that no matter what you do, you can always be hacked. Once you accept that, you can decide what level of cyberINsecurity that you can afford to live with and how much that you can spend to reduce the chances of being hacked. Then you can decide what steps you can afford to take in the event of a cyber-disaster. Cybersecurity procedures and a COOP are the perfect topic of discussion for a board working session or retreat. Stepping away from regular board business and playing "What If" is the first step towards a Lemonade and Chickens analysis. Cybersecurity doesn't have to be complicated and it doesn't have to be expensive.

Elizabeth M. Dietzmann is an attorney who consults with small utility systems on a variety of operational, financial and management issues. She can be reached at elizdietzmann@gmail.com or 573-578-1660.