Cybersecurity Tips for Water Utilities

Take these Steps to Help Keep Systems Safe

BY MATT PARKS, OHM ADVISORS

> *"With such advanced cyberattacks becoming a regular occurrence, those responsible for public utilities need to be aware of the risks and what can be done to mitigate them."*

Stories of hackers breaching business networks are on the rise – do the Facebook, Under Armour/MyFitnessPal, and Google system breaches last year ring a bell? The stories are real and they're rampant, and no-one wants it happening inside a community water or wastewater system.

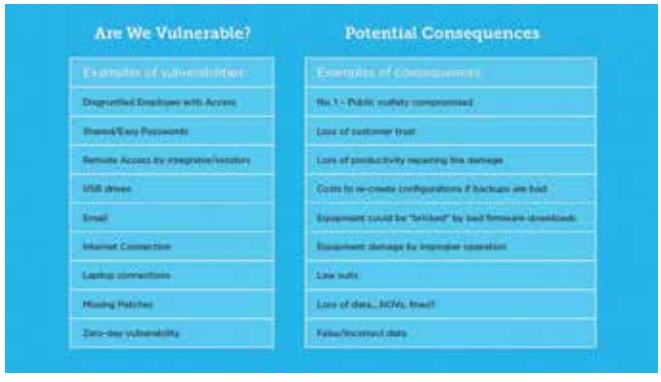
With such advanced cyberattacks becoming a regular occurrence, those responsible for public utilities need to be aware of the risks and what can be done to mitigate them. Simply ignoring technology is not a practical solution when we all have to 'do more with less.'

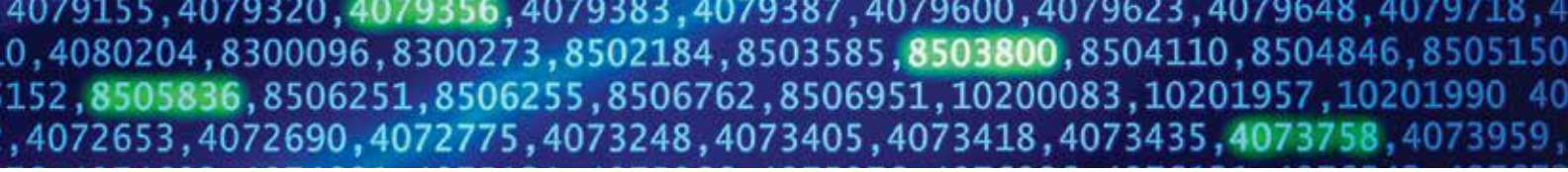
The US Department of Homeland Security considers water systems to be critical infrastructure. It is entirely possible that cyberterrorists could target vulnerabilities in US water and wastewater systems – and not just when they're connected to the internet. If laptops, USB drives, or other removable media are exposed to malware and then brought inside the firewall, it can put an entire system at risk. So, too, can something as seemingly innocent as using a cellphone to take a reading.

The impact of a water or wastewater system being compromised is significant, often to a much greater degree than compromising a business network. For a company, an attack can cost a lot of money. But with a water utility, if someone takes control of the network, it's not just money at stake – it's people's health, safety, and welfare.

That's why water utilities large and small must be vigilant in keeping their information systems – specifically the industrial control network or the process network – safe from outside intrusion. They must strive to maintain the integrity of their systems and ensure they remain available to the people who rely on them every day.

But how? Even though basic principles might be understood in most cases, there can be challenges in addressing those principles and placing a priority on cybersecurity, especially with smaller utilities who do not have budget for a full-time Chief Information Security Officer (CISO).





Here's some additional insight, with help from the Great Lakes Water Authority's Director of IT Security and Risk Management David Manor, on why it's so important for utilities of all sizes to increase their understanding of cybersecurity risks and take advantage of existing resources for help.

A Starting Point

A terrific resource to help utilities get a better grasp of the issues and start putting an action plan in place is the American Water Works Association. They offer an online tool[1] to address President Obama's 2013 Executive Order No. 13636 mandating improvements to critical infrastructure cybersecurity, as well as training on how to use the tool.

Of course, the question then becomes, who participates in the training? Inside large utilities like GLWA, which serves a customer base of more than 3.9 million people and puts significant effort into keeping its information systems safe from outside intrusion, there's dedicated staff to do the work.

But in many cases, smaller utilities don't have a full-time CISO for budget reasons, or because they simply have fewer systems and do not have the need or workload for one.

"In that case, even a sharp desktop support person can easily take simple first action steps to protect the system," Manor says. "Eliminating remote access to the system's network and ensuring that baseline security measures are in place is a must."

Next Steps

Manor says utilities can eliminate a major percentage of risk by implementing further basic steps, like making sure all systems are patched at least one a month and there's endpoint protection in place, beyond antivirus, to avoid network breaches that might come from security weak points – including potentially unprotected tablets, smartphones, and other wireless devices. Laptops and other mobile devices need to have protection for when they are outside the network, which is fairly easy to do, as with Cisco's steps for protecting mobile devices.[2]

For utilities that don't have these capabilities in house, some states – Michigan for example – offer CISO-as-a-service, where utilities can essentially get part-time help from a qualified IT professional. Communities receive a scorecard or assessment they can use to better understand and prioritize their risks. This scorecard leverages the state's free CySAFE[3] IT assessment tool.

The Department of Homeland Security also offers services[4] to help organizations prevent attacks by understanding their IT landscape, identifying their most critical needs, and creating plans to address them.

"One thing that utilities must keep in mind," Manor says, "is that cybersecurity is an ongoing process. They need to continually review their needs and make updates to keep their cybersecurity plans up to date. It's not just a one-and-done type of endeavor."

Overlooked or Misunderstood System Vulnerabilities

The most overlooked are often the most obvious, yet are straightforward to remediate: things like perimeter defense, such as firewalls and instruction detection, operating system patching and application patching, and endpoint protection including antivirus, firewalls, and intrusion detection on the endpoints. Also, it's vital to segregate the industrial control network so it cannot be accessed via the internet.

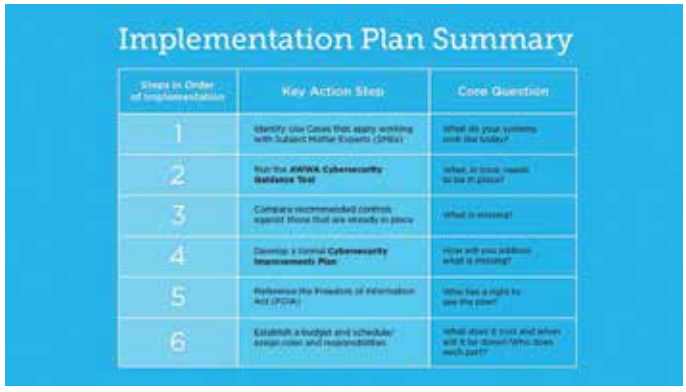
Manor says people tend to think these things are too difficult or too expensive to implement, and they're not. They can often be addressed by an in-house IT support person or a CISO-as-a-service resource. Utilities can also sign up for services that alert them to vulnerabilities and patches, and there are several options available online, such as those from the Department of Homeland Security's website.[5] The danger here, however, is information overload. Utilities will need someone to filter through the information and identify the priority issues – but if each of these items are checked off the list, most utilities will be in fairly good shape.

It's also necessary to watch out for emails that trick employees into clicking a link that gives a hacker has access to a community's system. It's a trickier issue, but preventable with free 'phishing' education for employees available online.[6]

Important Takeaways

Manor says that it's possible to have a good IT security program, regardless of the size of the water utility.

"Perhaps it's just a Word document that outlines what you do every day, every week, and every month. And that's perfectly acceptable for smaller utilities. The key is to stay informed and to take the reasonable measures – patching, endpoint protection, and network segregation – to protect your infrastructure."



There's help out there. With the excellent programs available from the Department of Homeland Security, the AWWA's cybersecurity tool and guidance, and the CySAFE program, cybersecurity is in reach for all utilities.

Resource Links:

[1] *www.awwa.org/resources-tools/resources/cybersecurity-guidance*
[2] *blogs.cisco.com/smallbusiness/protect-mobile-devices-protect-your-network*
[3] *www.michigan.gov/documents/cybersecurity/cysafe_flyer_som3_468548_7.pdf*
[4] *www.dhs.gov/cisa/critical-infrastructure-vulnerability-assessments*
[5] *www.us-cert.gov/ncas/alerts*
[6] *www.getcurricula.com/phishing-training/*