June 2019 - Vol. 35, Issue 6

ENDEAVOR BUSINESS MEDIA

WaterWorld®

Serving the Municipal Water/Wastewater Industry • www.waterworld.com

San Francisco's One Water Approach to Resiliency

Also Inside

Survey says: An informed customer is a happy one

Plant-based odor control

Water security: An insider's view

Special Section

Water Utility Management

Products & Services

Sludge processing & handling

Management software & systems

Unfiltered: An Insider's View of Water Security

Q&A with Steve Worley, SCADA security manager for the City of Raleigh, N.C.

BY MARC GENDRON

Steve Worley and the City of Raleigh, N.C., were honored in the seventh annual CSO50 Awards for their security initiatives. Photos courtesy of City of Raleigh.

The City of Raleigh, N.C., and Steve Worley, SCADA security manager, were recently honored in the seventh annual CSO50 Awards, which recognize 50 organizations (and the people within them) for security projects or initiatives that demonstrate outstanding business value and thought leadership. Worley is an advocate for improving water system cybersecurity and industry initiatives around information sharing and collaboration. In this Q&A, he shares his views on the state of water system security as well as his experiences and best practices for implementing measures to protect public utilities from cyber threats.

Q: *What is your role at the City of Raleigh?*

Steve Worley: I'm part of the City of Raleigh Public Utilities Department and we have a technical applications group as part of that department. My primary focus is SCADA security, which includes performing internal security assessments and external assessments, sometimes though the Department of Homeland Security (DHS). Based on our findings, and recommendations and action items that we develop with DHS, we are continuously working to increase the security posture for our SCADA network. We evaluate everything, the systems and network switches, the programmable logic controllers (PLCs), and try to conform to recommended architectures and practices to provide the best security possible.

Q: *What are you most concerned about or focused on in terms of security right now?*

SW: Like everyone else, we worry about external threats. Ransomware has made a lot of headlines in the past couple of years. Fortunately, we limit our exposure by keeping email off of our operational network and relegate that to the business network. In addition to external threats, we're also concerned about insider issues. Whether it's intentional, like somebody doing something they shouldn't do, or human error, which of course is unintentional. You can have accidental consequences that can cause problems, too. So, we try to look at all those scenarios.

Q: *What are the biggest challenges you see in terms of monitoring for those type of threats and detecting them?*

SW: Clearly, it's visibility. We've tried to increase our ability to monitor and that is one of the reasons we implemented a security product from a vendor called Indegy to be able to better monitor our network. We evaluated a number of tools, and one of the things that we like most about their technology is the active monitoring capability that allows us to actually query PLCs and see if changes have been made to them. Since changes can be made in a variety of different ways (over the network, directly on a device, etc.), in some cases they can be hard to detect. But if you query the PLC, then you can see if the code on that PLC has changed. The ability to not just monitor network traffic but also discover and inventory our devices, knowing all the systems and equipment that are on the network, was very important to us.

Q: *What advice would you give your peers in the industry that are struggling with the same problem?*

SW: The first thing I did when I started with the city was gather a detailed inventory of what systems were part of the network. This was initially done by just going out and putting hands on the systems. But with some of the automated tools that are available now a lot of that can be done in a matter of seconds by pulling information that's available on the network. For example, you can find out what version of Windows you have,

firmware levels on PLCs and other information. It's a lot easier than going out to every system and figuring out what firmware level you might have on a PLC.

Automation has been a big help and saved a lot of time. We're doing things in relation to logging and keeping things updated. All those are good best practices if you want to get things like Windows XP off your network, if you see any of that out there as part of your inventory and other systems that are out of support or might have known vulnerabilities. I try to keep up with the ICS-CERT advisories that come out and see if any of those apply to us. Tools that can identify code levels or firmware levels, known vulnerabilities, so they can be fixed, are extremely helpful.

Active monitoring allows the City of Raleigh to query PLCs and see if changes have been made.

Q: *Now that you've now been through the early days of implementing ICS security, what lessons did you learn that you would like to pass on?*

SW: I would definitely recommend automation. Things that would take hours or days to do, you can do in a matter of minutes in some cases. So, this is definitely important. Also, security should be a continual process. Once we complete one set of initiatives, we immediately have new initiatives that we're working on to continue to improve our security posture. Things change fairly quickly. There are always new threats and vulnerabilities, that require taking action to stay current and secure.

Security should be a continual process; once one set of initiatives is complete, utilities should begin working on new ones to continue to improve their security posture.

With automation, things that would have previously taken hours or days to do can sometimes be done in a matter of minutes.

In the water and other process-oriented sectors, industrial control systems (or operational technology [OT] as we call it) are designed and built to last 20, 30, 50 years. IT systems, on the other hand, are typically obsolete after five years, so you have to plan for that and have an update path. Our industry needs to be more engaged and knowledgeable in this area. For example, we can design a plant to run for 50 years, but the computer systems may be totally obsolete in five. We need to plan how we're going to keep those updated. Even though we're running OT environments, there is an IT component that we need to treat differently.

Q: *What future initiatives or plans are you looking at down the road with respect to OT security?*

SCADA Security Manager Steve Worley.

SW: One trend I'm seeing is the move to keep track of vendor security. So, in other words, the City of Raleigh works with a number of different vendors and we need to monitor their cybersecurity posture also. There are companies that rate the cybersecurity risk of third-party vendors using a credit-score model. That's of interest to us. If one of our vendors gets hacked, then that could jeopardize us in some way. We need to be concerned about that.

Q: *Are there any final thoughts you'd like to share that would be helpful for other water security professionals?*

SW: Yes, there are some great services provided by the Department of Homeland Security, which has several free services for water utilities and the wastewater industry where they will perform assessments. This information can be very helpful for making decisions on where to proceed with a cybersecurity program. **WW**

About the Author: Marc Gendron has more than 25 years of experience as a communications, media relations and analyst relations consultant focused exclusively on the B2B technology sector.