2022/4/23
Cyber Attacks

Cyber-Secure Water Supply

WT Interview with Graham Nasby, P.Eng, Water SCADA Specialist, City of Guelph Environmental Services

WT staff

The risk is always there, and this has to be carefully managed.
Graham Nasby, P.Eng. SCADA Specialist

WT: Graham, thanks for doing this. Can you explain to our viewers, what Cyber Security is, and why it matters for drinking water plants?

Graham Nasby: Cyber security is basically computer systems, how we keep them secure. We make sure that the people using them, are able to use them, so they have the functionality they need to do their jobs and deliver the services that we provide. We are also keeping out people that shouldn't be in the systems.

Obviously, the treatment of water is a critical service; we need to make sure all the equipment and computerized systems that run, are working properly. If we have any remote connections into control systems, we want to carefully filter out anyone that should not be connecting. We also want to keep data that we log, for billing, for proof of adequate treatment, records provided to the Ministry for our inspections, we want to make sure to preserve the data integrity complete.

We don't want to restrict this system, we don't want to have criminal organizations breaking in, putting a ransom in, locking up our data, We want to make sure there is no interference with the operation of the system. Guelph has multiple levels of safeguards in place, to be sure access is very carefully walled off so we can continue to produce the water we all depend on.

WT: When you talk about ransomware attacks, can you catch us up on these cyber-security terms?

Can you explain the different types of attacks and threats?

Nasby: Starting off with the one that most people are familiar with, the unauthorized access and copy of information. Any of you with a credit card or bank statement has probably experienced this at some point, getting a call from the bank that your card has been compromised, meaning there has probably been a point-of-sale terminal or banking machine, or something has gone wrong with the computer system. So, someone has gained access to your banking information or the login and password.

A more industrial example, one that did affect us a lot, last year there was a hack of a major gas pipeline, Colonial Pipeline. They provide gasoline to much of the east coast. In that attack, the hacker got in and encrypted a big portion of the computer system, to such a degree that Colonial couldn't run their pipeline for three weeks. This caused a lot of disruption because people couldn't get gasoline. That's an example of ransomware, where a system is being tied up.

Another type of attack is where a hacker breaks into an insurance company or health information company and is able to make an unauthorized copy of the data there. They will try to blackmail that company, and say "Hey if you don't pay this ransom money, we are going to release information of your customers". This attack is a breach of privacy information.

So those are three different types of attacks in the IT space.

It's criminal organizations doing these attacks. They figure there is a lot of money to be made if they can extort money out of organizations, with funds that are very hard to trace, such as cryptocurrency, and bitcoin.

In the OT space, which is what I do, Operational Technology, these are the systems that run our water supply, that track the amount of water used. A lot of the attacks on these systems interfere with how the system works. Access to the logs, the data or trying to lock the systems up. Now fortunately there have not been a lot of attacks like this.

In Guelph we have multiple levels of protection to prevent this type of access to our systems, in fact, some systems have no access at all, for this reason. Something to keep in mind, is we have to invest in (cyber-security) for our systems, that's why people get a water bill, it's not just for the water, we also have to protect these systems.

WT: Last year there were several incidents where water plant operations were affected, where the chemical mix needed to purify the water was changed; there are valves and pumps that can be accessed from outside the facility, so you could get tons more chlorine than there should be, or someone can turn up a pump or turn off a pump. Can you tell us more about that?

Nasby: One of the attacks you are probably referring to is the Oldsmar, Florida attack that occurred in February of 2021. In that case, they had an older, remote access connection, where staff can access the plant to make remote adjustments. The system was more than twenty years old. It had not been updated, patches had not been installed, and there were some current practices for cyber security they were not applying.

Also, not so great, the way that system was designed, it was possible to increase the dosage of chemicals to a very high rate. They were lucky, when that incident occurred, an operator was in the

control room and saw something funny happening on the screen, saw numbers changing, saw the mouse pointer moving around. He was able to shut down (the attack).

There was a similar incident in 2007, in Spencer, Massachusetts, where they had to issue an order for two days while they got the system flushed out.

So, the risks are there.

A lot of times when you are seeing incidents happen, it's usually a smaller utility that hasn't kept their systems up to date, may have got some outdated advice, and hasn't done a risk analysis.

In Ontario, for our operating permit we must do an annual risk analysis, and we have to keep these systems up to date. There are some parts of our system we don't allow remote access to because we have decided the risk is too high, but there are some areas with very carefully designed remote access. It's a live system, it's something we have to continually maintain.

WT: Can you explain, what is IT vs OT?

Nasby: IT, Information Technology, we are familiar with, this is the desktop computers, laptops, emails, websites, and often now includes phone systems, managed by IT. The focus is on information and data, and how that data moves around. Updates are done during the downtime.

OT stands for Operational Technology. This is a fairly new term in the industry; has only come into usage in the last three or four years. OT refers to the operational systems that run the equipment. An example would be a control system running pumps in a pumping station; that OT system must run all the time. A lot of OT systems may have only minutes of downtime in a year. Updating OT systems is challenging. Updates must be carefully planned, as you have to take that pumping station offline, do the updates, do the testing and bring it back online.

WT: When I look at water systems across the country, there are very many small cities with water treatment plants; I don't see a lot of programs for cyber security though. Do you know the percentage of these plants that may not be up-to-snuff on cyber security? Who does a water operator contact for help with cyber security?

Nasby: There are typically a couple of different categories of water utilities. We have the very old OT, typically no remote access, computer systems are quite limited, and are kept in locked buildings. So, the cyber risk there is fairly low.

We have another group that has some more modern systems. These may have some older remote access, and depending on how it is implemented, they might have a higher risk profile, but they may not.

We also have systems with fairly sophisticated, modern OT systems which will have remote access. Those systems are usually kept up to date.

The percentage (water utilities with unmanaged cyber risk) is hard to guess and always changing. Water utilities are inspected every year. There are a number of operational and maintenance plans that have to be filed, for regulations. Utilities are continually updating. Our regulator, the Ministry of

Environment, Conservation and Parks takes a proactive role in this.

For example, there is an initiative this year for cyber-security, and shoring up the utilities, this includes our inspection program with the Ministry.

It's an evolving area, you will see more utilities spending more money on cyber security because the threat is growing, it's something to keep an eye on, to manage that risk, to keep our water running.

WT: Ontario Water Agency (Aqua) has a contact email, if someone is concerned, or wants to know the security around their water plant or their information. Is this something every water plant should have, an email for the residents? How much should people be learning about this?

Nasby: I don't think there is any need for the public or customers to be concerned about this. We have a very stringent regulatory scheme in Ontario. Every water utility has an ORO, Overall Responsible Operator, that keeps an eye on the system, and ensures that all requirements are being met. All water operators in Ontario must be licensed, with continuing education credits required. There is a robust scheme for running the water space.

If a member of the public has a concern, they can always call customer service and find out more information. Utilities have an annual summary report, that would answer questions. I think we are in very good hands.

WT: If I am in a small town or medium-sized town and there has been a breach of the OT or IT systems, do they have to tell me? Do I get to know when there is a cyber-attack?

Nasby: Most utilities will do an assessment of what has happened and who is affected. The best practice is to notify the users. Most utilities have open and transparent communication of risks and concerns, any town would do that, and if not, questions should be asked.

WT: So it's not mandatory, no hard and set rule for disclosure of security breach?

Nasby: In the utility, I work for, we would notify our customers, if there was an issue.

WT: What are the next steps for water plants around cyber security? With AI, machine code, is there anything on the horizon that will change things radically for cyber security or will things go along as they have been?

Nasby: There is no silver bullet, every issue needs to be managed.

Artificial Intelligence is starting to be used, software used to monitor network traffic for unusual patterns and alert someone to look into it.

Any infrastructure water, gas, requires investment in its assets over time, buildings pipes pumps. The asset management program was brought in 2015, a change to the water industry regulation, look at the assets and keep them up to date. Cyber security is part of that.

WT: I introduced you as a Water and SCADA expert. Can you tell us what that means?

Nasby: Supervisory Control and Data Acquisition, is what SCADA system is. It is an automatic control

system I have been working with for over twenty years; I was happy to join the City of Guelph six years ago. This system generates alarms and alerts to contact the on-call operator if something does not look right.

WT: Thanks for doing this Graham.

Related info

- **A to Z**
- **Advisory Maps**

For articles published before 2020, please email or call us

Have a question? Give us a call 613-501-0175