ISA Water & Wastewater Industries Division

Protecting our Water/Wastewater Infrastructure – Identifying and Mitigating Cybersecurity Threats

by **GrahamNasby** on April 19, 2022 in **Articles**

Cybersecurity is an ever-growing threat to our critical water infrastructure. Recently, I had the pleasure of being part of a discussion panel that included Bryan Hurd from AON and Thomas Kuczynsk from DC Water at the *2022 National Water/Wastewater Conference*. Though each of us panelists gave presentations from a slightly different perspective, Bryan from a cross-industry perspective, Thomas from a large utility viewpoint, and myself from medium-sized Canadian utility, our message was the same. The cyber threat to our collective water infrastructure continues to grow and we all need to invest more into protecting our critical assets.

Identifying the Threat

Computerized systems play a centralized role in any water utility. These roles include customer management and billing, office IT systems, recording keeping, work order systems, fleet management software, compliance software, document control systems, communications systems, and automated control and monitoring systems. To ensure the efficient and safe operation of a water/wastewater utility, all of these various computerized subsystems need to be available, functioning properly, and securely interacting where required. Some of these subsystems can tolerate some downtown; however, many cannot. For example, while having email offline for short periods of time is an annoyance, automated control systems, such as the supervisory control and data acquisition (SCADA) systems that monitor and control water plants, cannot tolerate an outage of more than a few minutes.

Cyberattacks against the computer systems used at W/WW utilities generally fall into the following categories:

- **Denial of Service** – an attacker actively blocks access or consumes system resources, so the system is not available for its intended use.
- **Ransomware** – unauthorized encryption of data or servers, so that the system is not available for use and data is held hostage, until a ransom is paid.
- **Data Theft** – an attacker gains unauthorized access to they can copy data
- **Unauthorized Access** – an attacker gains unauthorized access to a system so that they can copy data or make changes at will.
- **Unauthorized Modifications** – an attacker gains unauthorized access to system, usually a SCADA system, so they can issue commands or change setpoints with the intention of damaging property or impacting human health.

The methods used by attackers to carry out these attacks are numerous, yet most can be traced back to Internet connectivity of some type. Often, an attacker is exploiting a known vulnerability associated connectivity to the Internet, but this is not always the case. For IT-based systems, which share networks with email systems, a common method used by attackers is to send fraudulent emails to a staff person to try to trick them into installing an attack program or opening access to a would-be attacker. This type of attack, called phishing, is one of the main reasons that IT departments now install aggressive anti-virus software and restrict administrative permissions on office computers. However, not all IT systems are fool-proof and new vulnerabilities continue to evolve due the rapidly developing world of software and remote connectivity. If there is a remote connection or Internet connectivity, there is always a potential attack vector that must be managed. With that said, one of the tried-and-true methods of infecting a computer system is to leave "free USB keys" in parking lots or as give-aways at conferences, so unsuspecting people will use them in their computers.

Cyber Threats are not new

The threat of cyberattacks on infrastructure is not new. Even as far back as in 1988, the *Morris Worm*, a computer attack originated by a student from Cornell, was estimated to have caused up to $10 million of damage in over 6000 servers[i]. A decade later, in 2000, a series a cyberattacks on sewer utility's SCADA system in Maroochy Shire, Australia resulted in 800,000 litres of raw sewage being intentionally discharged onto front lawns[ii].

Fast forward to the present and there are now (unfortunately) an increasing number of examples of water utilities being targeted by cyberattacks. In the past year (2021), there have been several notable attacks in the USA. Here is a sampling: In January 2021, a hacker tried to poison a water treatment plant in San Francisco Bay area[iii]. In February 2021, a hacker attempted increase to caustic soda feed rates to dangerous levels at drinking water plant in Oldsmar Florida[iv]. In March 2021, a Nevada-based water/wastewater utility's SCADA systems were ransomwared[v]. In May 2021, the SCADA network for a Pennsylvania water utility was breached[vi]. In July 2021, a hacker was able to completely disable a Maine-based wastewater plant's SCADA system[vii], and the plant had to be run in manual while the SCADA system computers were replaced.

Looking closer to home, while it is difficult to find publicly disclosed examples of attacks specific to Canadian water/wastewater (W/WW) utilities, there have been numerous attacks to municipal IT systems reported in the media during the past few years. These have included: Wasaga Beach (2018)[viii], Midland (2018)[ix], Stratford (2019)[x], Woodstock (2019)[xi], Metro Vancouver Transit (2020)[xii], and the Toronto Transit Commission (2021)[xiii], just to name a few. Based on unofficial anecdotal reports in the Canadian W/WW SCADA community, there have also been several municipal water/wastewater SCADA systems that have been compromised due to their connectivity to compromised IT systems. In each case, the utilities' SCADA servers had to be completely replaced and the facilities run in manual while repairs took place. From the above municipal cyberattacks, it is notable that several of the associated W/WW SCADA systems were not affected because they had no remote access or connection to IT systems.

A Growing Threat

Looking at cross-industry statistics, a staggering trend can be observed when it comes to cyberattacks – the frequency and costs associated with cyberattacks are rising at an exponential rate. According to a recent Ponemon/IBM study[xiv], the average cost of a cyberattack / data breach in Canada has risen to almost $4.5 million per occurrence. The global cost of cybercrime in 2018 was $600 billion worldwide, with that figure expected to rise to $2 to 6 trillion dollars in 2022. Just from ransomware alone, the global costs were expected to reach over $20 billion in 2021[xv].

But why is this the case? There are several contributing factors. The first and foremost is that for cyber criminals there is now a huge potential profit that can be made from attacking computer systems and holding them ransom, no matter the type of computer system. This is because businesses and critical utilities now use computer technology to such an extent that when these systems are taken offline, the negative impact provides a strong motivation for ransoms to be paid. Secondly, computer systems now are being connected with each other in so many ways that it provides a wide variety of avenues for cyberattacks to be carried out. Thirdly, with the rise of untraceable money transfer methods such a crypto currency, there are now much easier methods for cyber criminals to collect on ransom payments with little fear of being caught.

Furthermore, in our current age of global political unrest there are now also nation-state sponsored and funded cyber attackers who will now attack computer systems for a wide variety of political or ideological reasons. For example, in early 2022 alerts were recently issued by several Western governments warning W/WW utilities to increase their vigilance against cyber attacks motivated by the current tensions in the Ukraine.

We no longer live in an age where cyber attacks are being carried out by bored college students looking for a thrill – modern cyber attackers are now highly motivated, highly skilled, very well organized, and well funded. Several cyber security professionals are even now using terms such as “cyber crime for hire” or “ransomware -as-a service” where cyber attack tools can be easily purchased online by a would-be cyber attackers from a wide range of nation-state or criminal organizations.

Not a rosy outlook for sure, but fortunately, there are a wide variety of techniques and industry best practices that can be used by W/WW utilities to help protect themselves from the ever-growing menace of cyber attacks.

Countering the Threat

Fortunately, there are now a growing number of consensus-based technical standards and guidance documents available to assist utilities in protecting their systems against cyberattacks.

For IT systems, the ISO/IEC-27000 series of standards provides a comprehensive cybersecurity framework for managing IT infrastructure. The standards have a wide breadth, including privacy, authentication, information security, confidentiality, access control, and securing IT networks.

For OT systems, the ISA/IEC-62443 series of cybersecurity standards provides guidance specific for securing SCADA systems. Published by the International Society of Automation (ISA) and the International Electrotechnical commission (IEC), the 62443 standards are focused on meeting the high-availability and process control integrity requirements of SCADA systems, unlike the more data-centric focus of IT systems. The 62443 standards also provide guidance on how to securely implement remote access to SCADA systems, should that functionality be needed.

The American Water Works Association (AWWA) has also prepared the GW43014(R20) *Security Practices for Operational and Management”* standard and provides a water-industry specific cybersecurity risk assessment tool[xvi]

In Canada, Public Safety Canada has also been increasing active in the past several years with providing a wide range of tools and resources for critical infrastructure, including water/wastewater utilities[xvii].

Likewise in the United States, government bodies such as the Cybersecurity & Infrastructure Security Agency (CISA)[xviii], Department of Homeland Security (DHS)[xix], and National Institute of Standards and Technology (NIST)[xx] have been increasingly developing a wide range of resources for public water/wastewater utilities to use for hardening systems against the threat of cyber attacks.

Other national governments are now starting to provide similar resources and support for their respective countries. Cybersecurity is a global issue, and it is something that all utilities – regardless of size or location – need to address on an ongoing basis as part their operational plans and risk management strategies.

Cybersecurity Challenges

Like many aspects of our collective W/WW infrastructure, funding for cybersecurity programs continues to be a significant challenge for many utilities. Both IT and OT technology continue to evolve. Many utilities are having a hard time keeping up. In particular, this is difficult for smaller utilities, which do not have the same resources as larger utilities. The increasing frequency of cyber attacks on both IT and OT systems are evidence that more investment is needed to keep the W/WW sector secure.

Unlike traditional water utility assets like pumps, pipes and valves, IT and OT technology does not have a 40 to 50-year lifespan. In fact, most modern IT departments are now using a 3-4 year lifespan for IT physical assets, with even shorter lifecycles being used for IT-related computer software. SCADA systems are not much different. On the OT side, the best practices lifecycles for SCADA software and servers are slightly longer but not much. Best practice is that any SCADA software older than 5 years should be upgraded to ensure that it contains the latest cybersecurity patches and features.

With that said, due to lack of funding and resources to upgrade and replace these systems, there are still many utilities in our sector who are running Windows-XP based SCADA software for their operational systems. Windows XP, first released in 2021, was last sold in 2007 – more than 15 years ago. To put this in perspective, several years ago, Microsoft stopped providing support for Windows 7 including security patches, as Windows 7 is now considered operationally obsolete. Windows versions 10 and 11 are the only Windows versions currently being supported by Microsoft for production systems. This example should serve as a warning bell to our water/wastewater sector. Cybersecurity is a growing threat will require additional funding, staffing and resources to counter in an effective way, and these investments need to be ongoing to ensure the safety and security of the water/wastewater infrastructure that modern society depends on.

Key Take-Aways

For the municipal W/WW sector, cybersecurity is an ever-growing threat that needs constant attention and vigilance to protect our computerized systems, whether it be IT systems or the process-control focused OT systems that are used by operations. Both IT and OT systems are critical systems for our municipal W/WW infrastructure that need to be adequately funded, keep up to date, and protected.

About the Author

Graham Nasby, P.Eng., PMP, CAP manages the SCADA system for public drinking water utility located in Southwestern Ontario. He is co-chair of the ISA112 SCADA systems management committee, and a member of ISA99 standards committee that develops and maintains the ISA/IEC-62443 series of cybersecurity standards. Graham is also a past-director of the ISA Water/Wastewater Industry Division. He lives in Guelph, Ontario, Canada and can be contacted at graham.nasby@grahamnasby.com

References

[i] https://www.kaspersky.com/blog/morris-worm-turns-25/3065/

[ii] https://www.theregister.co.uk/2001/hacker_jailed_for_revenge_sewage/

[iii] https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206

[iv] https://www.zdnet.com/article/hacker-modified-drinking-water-chemical-levels-in-a-us-city/

[v] https://therecord.media/us-govt-reveals-three-more-ransomware-attacks-on-water-treatment-plants-this-year/

[vi] https://www.wtae.com/article/fbi-investigating-hacking-threats-at-pennsylvania-water-systems/36386504

[vii] https://www.cisa.gov/uscert/ncas/alerts/aa21-287a

[viii] https://www.cbc.ca/news/canada/toronto/small-ontario-towns-pay-ransom-after-hackers-hold-computer-systems-hostage-1.4826545

[ix] https://www.cbc.ca/news/canada/toronto/small-ontario-towns-pay-ransom-after-hackers-hold-computer-systems-hostage-1.4826545

[x] https://kitchener.ctvnews.ca/stratford-paid-75-091-to-end-recent-cyber-attack-1.4601497

[xi] https://www.woodstocksentinelreview.com/news/local-news/cyber-attack-costs-woodstock-more-than-660k-report

[xii] https://bc.ctvnews.ca/printed-ransom-note-asked-translink-for-7-5-million-in-december-cyberattack-1.5389170

[xiii] https://www.itworldcanada.com/article/toronto-transit-commission-still-recovering-from-ransomware-attack/463683

[xiv] Ponemon/IBM Institute "Cost of a Data Breach Study 2020"

[xv] "Protecting today. Safeguarding tomorrow.", AON. Jan 18, 2022.

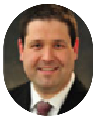
[xvi] https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance/

[xvii] https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/

[xviii] https://www.cisa.gov/

[xix] https://www.dhs.gov/topics/cybersecurity

[xx] https://www.nist.gov/cyberframework



About GrahamNasby

Graham Nasby, P.Eng., PMP, CAP is a project manager and automation engineer who lives in Guelph Ontario Canada where he is the Water SCADA & Security Specialist for City of Guelph Water Services. Graham was general chair of the 2012 and 2013 ISA water/wastewater symposiums, and is currently the editor of the ISA Water/Wastewater newsletter. He can be contacted at www.grahamnasby.com

View all posts by GrahamNasby →

Related Posts:

- 2018 ISA WWAC Symposium – Training

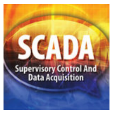
‹ Dates of 2022 Energy & Water Automation Conference webinars announced – Jun 14, Jul 19, Aug 16, 2022

Search...

Recent Posts

- Protecting our Water/Wastewater Infrastructure – Identifying and Mitigating Cybersecurity Threats

Cybersecurity is an ever-growing threat to our critical water infrastructure. Recently, I had the pleasure of being part of a discussion panel that included Bryan Hurd from ...



- Dates of 2022 Energy & Water Automation Conference webinars announced – Jun 14, Jul 19, Aug 16, 2022

The ISA Water/Wastewater Industry Division is pleased to announce the dates for our 2022 webinars for the virtual Energy & Water Automation Conference. The 2022 EWAC ...

- ISA112 co-chair Graham Nasby to host Q&A session on Tues, Apr 26, 2022 about the ISA112 SCADA Systems Management Lifecycle

Please block your calendars for Apr 26, 2022 for the ISA WWID ConnectLive meeting on ISA112 SCADA Standard – Part 2. 7:30am Pacific 8:30am Mountain 9:30am Central 10:30am ...

- 2022 ISA water/wastewater division Student Scholarship Winners Announced

The ISA Water & Wastewater Industries Division (WWID) is pleased to announce the winners of the 2022 WWID Student Scholarships. The scholarships are given out to promote ...

- Winter 2022 Newsletter now available online – ISA Water/Wastewater Division

The ISA Water/Wastewater Industry Division is pleased to announce that our Winter 2022 newsletter is now available on our division website at www.isawaterwastewater.com and ...

ISA International News

- 28 April is International Automation Professionals Day!
- Key Factors of Wireless Real-Time Networks: From Dependability to Timeliness
- What Makes a Factory a Smart Factory?
- How Can We Improve Control Loops with Slow Signal Updates?
- Check Out These 10 Podcasts on Automation!