ISTOCK.COM/URUPONG

# CYBERSECURITY AND OUR MUNICIPAL WATER INFRASTRUCTURE: IDENTIFYING AND MITIGATING THE THREAT

BY GRAHAM NASBY

Cybersecurity is an ever-growing threat to our critical water and wastewater (W/WW) infrastructure, which we all need to play a part in managing. 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.

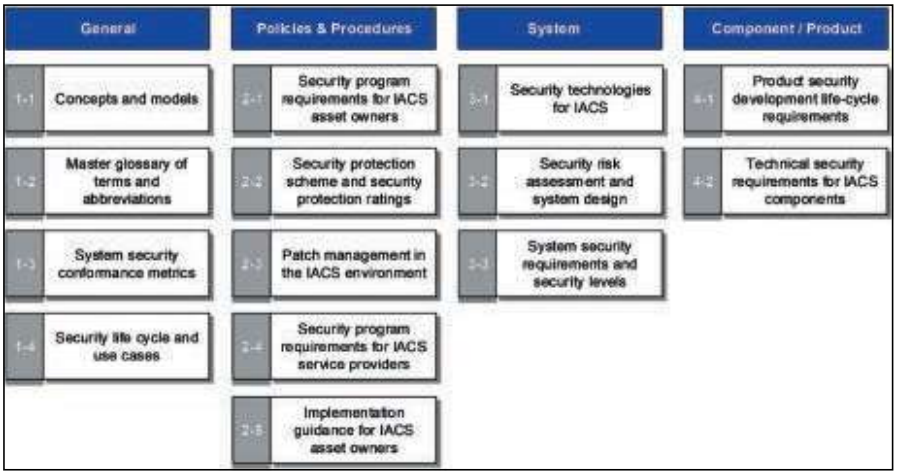
## Cyber Threats are Not New

The threat of cyber-attacks 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 computer servers.[1] A decade later, in 2000, a series a remote 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.[2]

Fast forward to the present and there are now (unfortunately) an increasing number of examples of W/WW 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 the San Francisco Bay Area.[3] In February 2021, a hacker attempted increase to caustic soda feed rates to dangerous levels at a drinking water plant in Oldsmar Florida.[4] In March 2021, a Nevada-based water/wastewater utility's SCADA systems were ransomwared.[5] In May 2021, the SCADA network for a Pennsylvania water utility was breached.[6] In July 2021, a hacker was able to completely disable a Maine-based wastewater plant's SCADA system,[7] and the plant had to be run by hand while the SCADA system computers were replaced.

Looking closer to home, while it is difficult to find publicly disclosed examples of attacks specific Canadian 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)[8], Midland (2018)[9], Stratford (2019)[10], Woodstock (2019)[11], Metro Vancouver Transit (2020)[12], and the Toronto Transit Commission (2021)[13], just to name a few. However, based on unofficial anecdotal reports in the Canadian W/WW SCADA community, there have been several municipal W/WW 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 operated in manual while repairs took place. In several of the above municipal cyber attacks, 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.

To put some additional perspective with the additional risks posed by a compromised SCADA system: In 2007 there was a malfunction in a SCADA system at a water utility in Spencer Massachusetts where the setpoint for caustic soda chemical feed pump was changed, which caused the drinking water pH to spike.[14] The incident resulted in 140 hospitalizations and a *do not consume order* being issued by the water regulator for 2 days while the town's entire water distribution system had to be manually cleaned.[15] In 2018, a similar type of SCADA malfunction was discovered in Hamilton Ontario, which had caused 24 billion litres of raw sewage to be discharged into Chedoke Creek during the previous 4 years period before someone noticed.[16,17]




## The Growing Cybersecurity Threat

Looking at cross-industry statistics, a staggering trend can be observed when it comes to cyber-attacks – the frequency and costs associated with cyber-attacks are rising at an exponential rate. According to a recent Ponemon/IBM study[18], the average cost of a cyber-attack/data breach in Canada has risen to almost $4.5 million per occurrence, and the global costs 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.[19]

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 "cybercrime for hire" or "ransomware -as-a service" where cyber-attack tools can be easily purchased online by a would-be cyber attacker 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

Compared to a few years ago, there is now a growing body of knowledge and industry best practices available to guide W/WW utilities in protecting their systems from cyber-attacks. This body of knowledge is available as consensus-based published standards and technical reports, specialty cybersecurity providers, and resources from government entities, such as Public Safety Canada and the Canadian Centre for Cyber Security. From a utility perspective, it is important that industry best practices, and specifically those developed for critical infrastructure, be used as much as possible rather than trying to develop an independent approach. Very few utilities will have the in-house knowledge to be able to develop a cybersecurity strategy without using these outside resources.

What follows is some general guidance of where to find these industry resources and how to start applying them.

## Securing Utility IT Systems

For protecting IT systems, there is a base set of cybersecurity standards called the ISO/IEC-27000 series that provide a comprehensive framework for how to manage the information security management aspects of IT systems. The scope of these standards (often referred to as ISO27K) is very broad in nature and covers almost every aspect of IT systems when it comes to privacy, authentication, information security, confidentiality, access control, and securing IT networks. Taken together a package, the ISO27K series of standards provides a comprehensive set of industry best practices when it comes to managing and securing IT systems. In terms of applying ISO27K, there can be wide variation for a utility depending on how its IT systems are managed, as some utilities may look after IT internally, rely on a parent municipality for IT services, or contract out these services to a third party. Regardless of how IT services are being provided, it's important that the guidance in ISO27K be followed and be continually updated as the standard evolves.

Some of the system hardening techniques that come from the ISO27K series include frequent password changes, minimum requirements for password strength, removing unused accounts, limiting access to systems to only those who need it, centralized account management, multi-factor authentication, segmenting networks into access zones, email filtering, cybersecurity awareness training, placing firewalls between IT systems and the Internet, multi-level encryption/authentication for remote access, and securing wireless networks, just to name a few.

IT systems now perform a wide variety of roles in modern W/WW utilities, so it is important that IT systems are designed to be both secure and service the utility's core business needs. A common watch-out for IT systems is to continually ensure they are designed around business needs so that users are not tempted to use insecure methods as workarounds to get their day-to-day work done.

## Securing Utility OT Systems

Operational Technology, known as OT, is a relatively new industry term used for SCADA systems and other high-uptime operationally-focused computer systems. Because it pairs well with the IT acronym, the OT term is now increasingly being used in the industry instead of referring to SCADA systems directly. For the purposes of this article, the terms OT and SCADA will be used interchangeably.

Unlike IT systems, OT systems have a very different set of requirements when it comes to uptime and availability. Whereas IT systems usually only need to be online during business hours, OT systems – because they are monitoring and controlling actual process equipment – typically cannot be offline for more than a few minutes at a time. OT systems also look after critical tasks such ensuring the safe/effective treatment of drinking water and monitoring water as it leaves facilities, so ensuring they are online is of paramount importance.

Thus, to contrast IT systems and OT systems with each other: An IT system will generally be focused around the privacy and confidentiality of data and some outages are usually acceptable. Whereas, an OT system will be focused entirely around uptime and availability and ensuring process control functions are always functional. Put another way, IT systems are usually expected to have an uptime of 90-95% (18 to 36 days of cumulative downtime per year), whereas OT systems such as SCADA are typically expected to have uptimes exceeding 99.99% per year (only 5 to 10 minutes of downtime per year).

Because of these unique needs, there are a separate set of cybersecurity standards documents for securing OT systems, known as the ISA/IEC-26443 series of standards. Entitled, "Security for Industrial Automation and Controls Systems," the ISA/IEC-62443 series of standards address the unique challenge of securing OT systems in critical applications. Like the ISO27K standards, the IEC/IEC-62443 series of standards are all-encompassing, but unlike ISO27K it is focused entirely on the unique needs of OT systems.

## ISA/IEC-62443 in a Nutshell

The ISA/IEC-62443 series of standards are a product of the ISA99 cybersecurity

committee, which is a multi-industry consensus-based technical committee hosted by the International Society of Automation, a non-profit technical society for SCADA professionals from around the world. The various individual ISA/IEC-62443 standards themselves are published by the ISA and the IEC, with the IEC version also being available in French.

In development since 2002, the ISA/IEC-62443 series of standards consist of four main groupings of documents focused around: General Concepts, Policies & Procedures, System Management and Component/Product Requirements. These are broken down further, as shown in Figure 1, into various guidance documents covering different aspects of how to keep SCADA systems secure.

Major themes present in the ISA/IEC-26443 include securing SCADA systems in terms of defining a required security level, developing a security maturity level of SCADA assets, and using a security lifecycle for managing security assets. Core principals involve securing the OT lifecycle, providing guidance to OT vendors and system integrators, guidance to the vendors on providing secure equipment, and dividing the SCADA system into zones that are only accessible via tightly controlled "conduits" for access.

A major principal of the ISA/IEC-62443 series of standards is to restrict access only to what and whom the minimum operational information is needed. This includes carefully reviewing the pros and cons of secure remote access in terms if it is actually needed from a work tasks point of view and how it can be provided to not introduce unacceptable risk. For example, ISA/IEC-62443 clearly states that SCADA systems must be kept separate from IT systems in order to ensure the integrity of the SCADA system, and interaction between the systems must be strictly controlled. Depending on the risk level, it may be advisable to have no IT connections to a SCADA system whatsoever. However, if remote access is needed, the ISA/IEC-62443 standards provide guidance on securely implementing remote access it to minimize the risk of a cyber-attack.

Some of the best practices from applying ISA/IEC62443 to SCADA systems include: separating SCADA systems in different zones with varying levels of access, ensuring SCADA systems are kept separate from IT systems, using multi-factor authentication and individual passwords for SCADA systems, encrypting and monitoring traffic on SCADA networks, ensuring SCADA systems have effective backup and disaster recovery systems, implementing configuration/code version control systems, implementing increasing logging/alerting of setpoint changes, and restricting who has access, and the level of access, to these systems. ISA/IEC-62443 also recommends having a strong policy and procedures framework for managing SCADA system security, and the SCADA system security be audited and tested on a regular basis.

The ISA/IEC-62443 series of standards also suggest taking a careful look at remote access requests to SCADA systems. The ISA/IEC-62443 standards view remote access as a potential attack vector that must be carefully managed and restricted, and if it is provided, will require ongoing resources to set up and maintain. Based on the approach recommended by ISA/IEC-62443 and current risk threat, some utilities have made the decision to not implement remote access to their SCADA systems, as it reduces their cybersecurity risk footprint.

The core message of ISA/IEC-62443 is that cybersecurity is something that needs to be designed into architecture of OT systems and it requires continual updates and monitoring to be effective.

## Water Industry Specific Guidance

In addition to the above specific guidance when it comes to IT systems and OT systems, the American Water Works Association (AWWA) has also prepared several technical guidance documents to help W/WW utilities navigate the everchanging cybersecurity threat landscape.

These include the GW43014(R20) *Security Practices for Operational and Management"* standard and the GW440-17 *Emergency Preparedness Practices* standard. The AWWA also now has a water-utility specific cybersecurity risk assessment tool, which can be found online on the AWWA website.[20]

The National Institute of Standards and Technology (NIST) in the United States has also prepared a cybersecurity framework for critical utilities that is now available on their website.[21] NIST also now has the NIST SP 800 series of cybersecurity guidance documents that provide guidance on how to implement ISO/IEC-2700, ISA/IEC-62443 and other related cybersecurity standards.[22]

## Canadian-Specific Resources

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 W/WW utilities. These now include checklists of cybersecurity resilience, a Canadian cybersecurity risk assessment toolkit, and regular industrial control systems security events.[23]

The Canadian Standards Association, through its CSA P125 Technical Committee on Operational Technology Functional Safety and Security, is also midst of adopting the ISA/IEC-62443 series of cybersecurity standards to be an official Canadian cybersecurity standard for automated control systems.

## Cybersecurity Challenges

Like many aspects of our collective W/WW infrastructure, funding for cybersecurity programs continues to be a 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 to 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

ESL Utility & Municipal Products

# SUPPLYING PRODUCTS THAT HELP UTILITIES GET WATER FROM THE SOURCE TO THE TAP

1-800-268-8309 • WWW.EVANSUPPLY.COM

NEPTUNE TECHNOLOGY GROUP
AUTHORIZED DISTRIBUTOR

- WATER METER SUPPLY
- WATER METER INSTALLATION SERVICES
- WATER METER READING SERVICES
- WATER METER TESTING SERVICES
- HIGH RESOLUTION ENCODERS
- PD, TURBINE, COMPOUND ULTRASONIC
- RF & CELLULAR TRANSMITTERS
- WALK-BY, DRIVE-BY, FIXED-BASE RECEIVERS
- CLOUD SOFTWARE

FORD METER BOX

- PIPE REPAIR CLAMPS
- EMERGENCY PIPE REPAIR KIT
- PIPE RESTRAINT
- PIPE COUPLING
- NO LEAD BRASS
- WATER METER PITS

KUPFERLE

- INTELLIGENT ALL SEASON FLUSHERS
- INTELLIGENT PORTABLE FLUSHERS
- STAINLESS STEEL SAMPLING STATIONS
- MANUAL BLOW OFF HYDRANTS


Palintest
Water Analysis Technologies

- CHLORINE TESTING SOLUTIONS
- LOW AND HIGH RANGE
- SENSOR OR DPD TECHNOLOGY
- KEMIO MULTI PARAMETER TESTING
- CHLORMETER DUO

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.

## 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.

## Cybersecurity Resources

- **ISO/IE-27000 IT Information Security Management Systems** – www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards
- **ISA/IEC-62443 Security for Industrial Automation and Controls Systems** – www.iec.ch/blog/understanding-iec-62443 and https://gca.isa.org/isagca-quick-start-guide-62443-standards
- **AWWA Cybersecurity Guidance** – www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance
- **NIST Cybersecurity Framework** – www.nist.gov/cyberframework
- **NIST SP 800 Cybersecurity Standards** – www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information
- **Public Safety Canada – Critical infrastructure** – www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr

## About the Author

**Graham Nasby, P.Eng., PMP, CAP,** *manages the SCADA system for a 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. He lives in Guelph, Ontario, Canada and can be contacted at graham.nasby@grahamnasby.com.*

## Sources:

1. www.kaspersky.com/blog/morris-worm-turns-25/3065/
2. www.theregister.co.uk/2001/hacker_jailed_for_revenge_sewage/
3. www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206
4. www.zdnet.com/article/hacker-modified-drinking-water-chemical-levels-in-a-us-city/
5. https://therecord.media/us-govt-reveals-three-more-ransomware-attacks-on-water-treatment-plants-this-year/
6. www.wtae.com/article/fbi-investigating-hacking-threats-at-pennsylvania-water-systems/36386504
7. www.cisa.gov/uscert/ncas/alerts/aa21-287a
8. www.cbc.ca/news/canada/toronto/small-ontario-towns-pay-ransom-after-hackers-hold-computer-systems-hostage-1.4826545
9. www.cbc.ca/news/canada/toronto/small-ontario-towns-pay-ransom-after-hackers-hold-computer-systems-hostage-1.4826545
10. https://kitchener.ctvnews.ca/stratford-paid-75-091-to-end-recent-cyber-attack-1.4601497
11. www.woodstocksentinelreview.com/news/local-news/cyber-attack-costs-woodstock-more-than-660k-report
12. https://bc.ctvnews.ca/printed-ransom-note-asked-translink-for-7-5-million-in-december-cyberattack-15389170
13. www.itworldcanada.com/article/toronto-transit-commission-still-recovering-from-ransomware-attack/463683
14. www.telegram.com/story/news/local/north/2007/09/06/dep-fines-town-34k/52801600007/
15. www.controlglobal.com/blogs/unfettered/water-control-system-cyber-incidents-are-more-frequent-and-impactful-than-people-are-aware/
16. www.hamilton.ca/government-information/chedoke-creek-spill-remediation-activities
17. https://globalnews.ca/news/6200239/hamilton-public-works-glitch-chedoke-creek-sewage-spill/
18. Ponemon/IBM Institute "Cost of a Data Breach Study 2020"
19. "Protecting today. Safeguarding tomorrow.", AON. Jan 18, 2022.
20. www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance
21. www.nist.gov/cyberframework
22. www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information
23. www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr