FEATURE

Cybersecurity and Our Municipal Water Infrastructure: Identifying and Mitigating the Threat

ISTOCK.COM/INCREDIVFX

By Graham Nasby, P.Eng., PMP, CAP

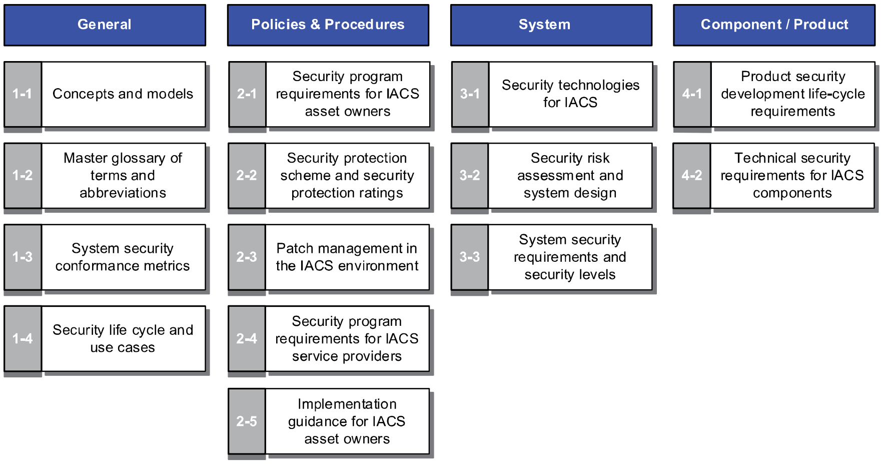
CYBERSECURITY IS AN EVER-GROWING THREAT to our critical water infrastructure. Recently, I had the pleasure of being part of a discussion panel that included Bryan Hurd from AON and Thomas Kuczynsk from DC Water at the 2022 National Water/Wastewater Conference. Though each of us panelists gave presentations from a slightly different perspective—Bryan from a cross-industry perspective, Thomas from a large utility viewpoint, and I from a 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.

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 6,000 servers.[1] A decade later, in 2000, a series of cyberattacks on a 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 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.[3] In February 2021, a hacker attempted increase the caustic soda feed rates to dangerous levels at 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 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)[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. 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.



General	Policies & Procedures	System	Component / Product
1-1 Concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Product security development life-cycle requirements
1-2 Master glossary of terms and abbreviations	2-2 Security protection scheme and security protection ratings	3-2 Security risk assessment and system design	4-2 Technical security requirements for IACS components
1-3 System security conformance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 Security life cycle and use cases	2-4 Security program requirements for IACS service providers		
	2-5 Implementation guidance for IACS asset owners		

Figure 1 – ISA/IEC-62443 series of cybersecurity standards for OT 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[14], 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.[15]

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 (Figure 1) 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.[16]

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.[17]

Key Take-Aways

For the municipal water/wastewater sector, cybersecurity is an ever-growing threat that needs our constant attention. Both IT and OT systems are critical systems for our municipal water/wastewater infrastructure that need to be adequately funded, keep up to date, and protected.

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. He lives in Guelph, Ontario, Canada and can be contacted at graham.nasby@grahamnasby.com.

References

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. 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-1.5389170
13. www.itworldcanada.com/article/toronto-transit-commission-still-recovering-from-ransomware-attack/463683
14. Ponemon/IBM Institute "Cost of a Data Breach Study 2020"
15. "Protecting today. Safeguarding tomorrow.", AON. Jan 18, 2022.
16. www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance/
17. www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/