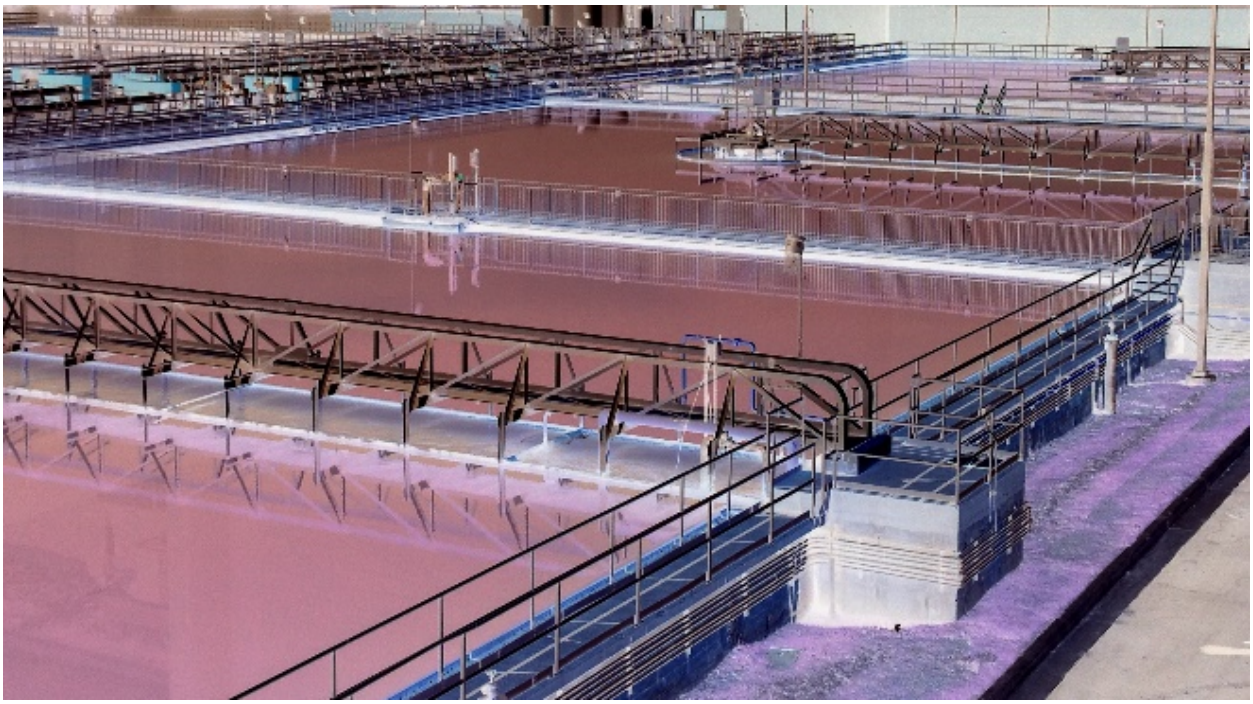
## The State of Cybersecurity in the Water/Wastewater Market

By Steve Murphy

*Water and Wastewater Industrial Control Systems (ICS) are under attack just as other critical infrastructure in our nation is. The number of attacks has increased significantly each year with more successful infections being reported. In this article we will discuss the state of water/wastewater control systems and the impact that the failure of these programmable logic controllers (PLC) and supervisory control and data acquisition (SCADA) systems has on water quality. We all want clean water that we can trust to drink, bathe and cook our meals with, but our dependence on technology has put water quality at stake as cyberattacks grow in number and potency every year.*

### People, Process, Technology

Traditionally, ICS have not placed much importance on cybersecurity protection, but due to the recent increase of virus, malware, and hackers' attacks, more attention is being paid to how our water sector ICS systems are being protected from cyberattacks. As we begin to discuss the subject of cybersecurity, it is important to consider people, process, and technology. These are three common areas of focus with regard to cybersecurity that help ensure a quality security program. Today's TECHNOLOGY provides numerous methodologies to aid in protecting a system from a cyberthreat, but no technology is bulletproof. PEOPLE are also key to a successful program. The users of the systems must be engaged in the overall program. People need not only proper training in the use of the system, but also awareness training of cybersecurity as a whole to ensure they understand the dos



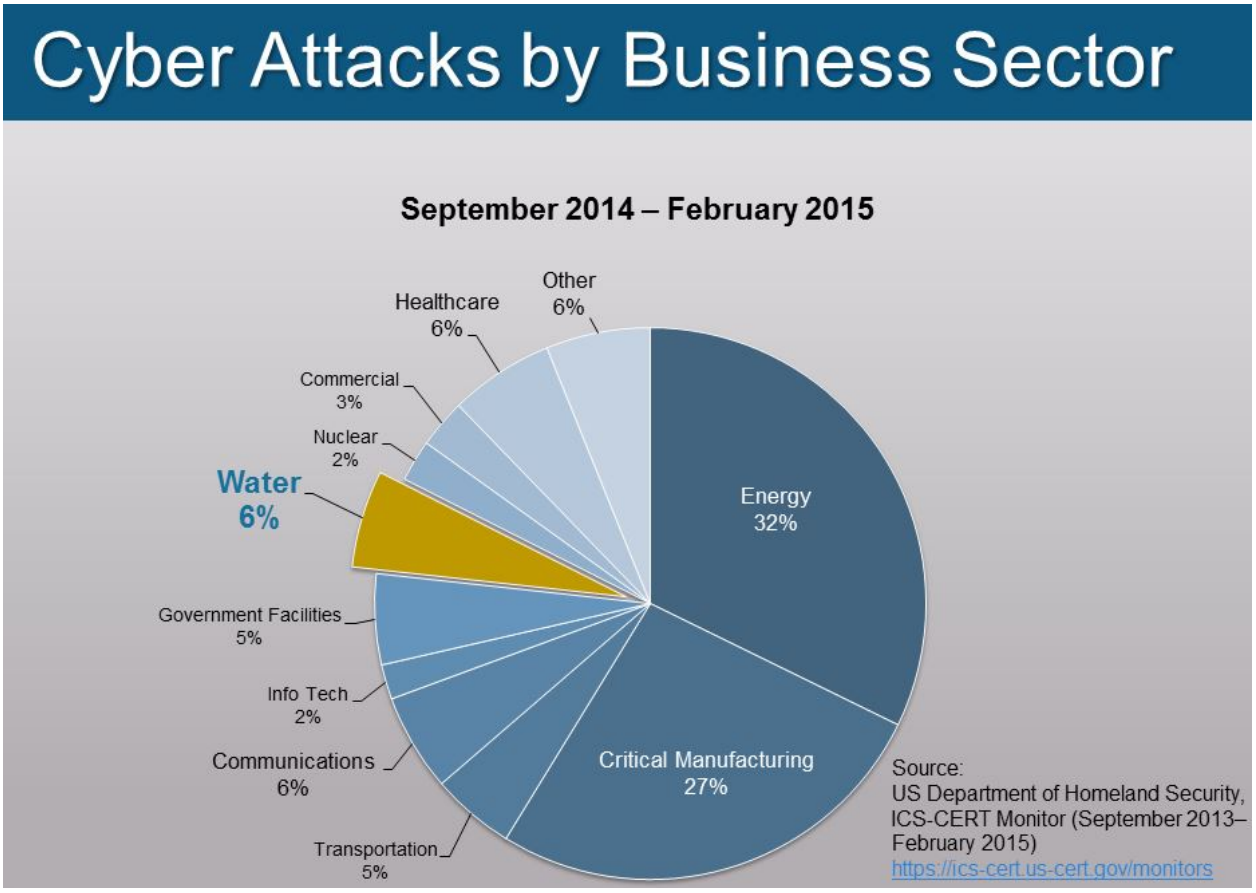
and don'ts of using the system and the things to watch for as they are using it. Finally, PROCESS is also a key element. This category represents the policies and procedures that must be put in place so that all users have a documented methodology to follow and through which to report.

## Historical Perspective

Over the years, control systems placed little focus on security. After all, they were controlling a process, not protecting data. Until recently, the biggest concern was an insider threat. This changed in 2010 when the world learned about the Stuxnet worm. Stuxnet is a malicious computer worm that specifically targeted ICS. It caused the physical destruction of nuclear centrifuges in Iran.

## Past Cyberattacks by Business Sector

The Department of Homeland Security (DHS) sponsors ICS-CERT (Industrial Control System – Cyber Emergency Response Team). ICS-CERT collects incident reports from ICS facilities and conducts assessments if requested. In 2009, only three events targeting the water and wastewater sector were reported to ICS-CERT.[1] It is likely that many other cases go unreported. The chart below shows a breakdown of cyberattacks by business sector dating back to 2014. The




[1] "ICS-CERT Incident Response Summary Report," ICS-CERT, 2009, https://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20%282009-2011%29_S508C.pdf.

Water Industry represented 6% of the attacks in this chart.[2]

In 2015, DHS investigated almost twice as many cyberattacks as the previous year with regards to the industries that support the nation's critical infrastructure. A total of 97 digital attacks occurred, with 25 of these specifically targeting the water and wastewater sectors.[3]

## Recent Water Sector Cyberattacks

Increased malware threats have also received more attention in the industry. As individuals, we are constantly bombarded with malware threats that can wreak havoc in our lives. These threats can result in crashing our systems, identity theft, and disabling the very components on which we rely. Control systems are not immune to this. The need to secure the data and components on control system networks is becoming more prevalent as malware concerns and hacking incidents have intensified. Therefore, beyond hardware issues, cybersecurity initiatives must also be considered. Historically, ICS networks were based on proprietary protocols and had limited security options. These systems were built with an emphasis on treatment processes. Conversely, business networks emphasized protecting data, thus had greater built-in security features. Solutions that worked well in the information technology (IT) environment are now more commonly used in the operations technology (OT) environment of control systems to better address cyber concerns.

## Ransomware

One of the scariest and most prevalent threats is ransomware, also known as digital kidnapping, a type of malicious software that encrypts users' documents and data. Perpetrators of these attacks demand ransom payments to unencrypt the data, usually requesting payment through a cryptocurrency such as Bitcoin. However, in a recent confidential meeting a FBI agent cautioned against paying these ransoms as there is no guarantee the criminals will provide the encryption key to restore files because only 10% of victims who paid have been successful in this regard. In 2016, ransomware infected nearly 40% of all businesses. In 2017, Malwarebytes reported that ransomware attacks increased to 90% against businesses, with attackers charging less Bitcoin to unlock users' files in hopes to getting more victims to pay.[4]

Several water utilities have reported ransomware attacks in recent years, and many more go unreported for fear of raising customer concerns. In April 2016, the corporate network for the Board of Water and Light (BWL) in Lansing, Michigan was affected by ransomware when an employee

[2] "ICS-CERT Monitor September 2014 - February 2015," ICS-CERT, March 11, 2015, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.

[3] Cory Bennett,"DHS: Cyberattacks on critical manufacturing doubled in 2015," The Hill, January 15, 2016, http://thehill.com/policy/cybersecurity/266081-dhs-critical-manufacturing-cyberattacks-have-nearly-doubled.

[4] Malwarebytes Annual State of Malware Report Reveals Ransomware Detections Increased More Than 90 Percent," Malwarebytes, January 25, 2018. https://press.malwarebytes.com/2018/01/25/malwarebytes-annual-state-malware-report-reveals-ransomware-detections-increased-90-percent/.

unknowingly opened an e-mail with an infected attachment. The malware caused the BWL's accounting and e-mail systems to shut down, though officials reported there was no evidence that personal information of their customers or employees was compromised. According to news reports, the city spent a total of $2.4 million addressing this ransomware attack, between virus removal on the entire business network and a payment of $25,000 in Bitcoin to unencrypt and retrieve the files. Fortunately for the local residents, the electric and water ICS networks were not affected; therefore, service was not disrupted. However, this type of attack on a utility demonstrates the potential danger of malware causing serious operational problems, especially if the IT and OT networks are interconnected.[5]

Another example of a ransomware attack occurred in early 2017 at the Mountain Home Water Department in Arkansas.[6] Based on the forensic analysis performed by the utility, the malware encrypted 90,000 files on the server in approximately 90 seconds. It appeared that all files that were not already open at the time of the attack were encrypted by the malware. Fortunately, the utility was vigilant and water department employees were immediately alerted. The utility was able to find an e-mail address within all encrypted files that could be used to communicate with the hacker. However, rather than negotiate a ransom to unencrypt the files, the server was erased and its data was recovered and reinstalled from a recent backup. In this case, the utility's contingency planning paid off as their normal procedures were to perform partial nightly backups and full weekly backups.

While neither of these ransomware cases involved the ICS network, a cryptocurrency mining attack successfully infiltrated the network of a water utility in Europe earlier this year after a human-machine interface (HMI) computer using Windows XP was exposed to a malicious advertising site.[7] The incident was discovered during a routine analysis by a third-party antivirus vendor, which found the utility's SCADA server to be mining Monero cryptocurrency. Although the presence of the malware cryptocurrency mining algorithm did not stop SCADA operations from functioning properly, operations staff had noticed a slowdown in the system. These events magnify the importance of performing frequent updates of operating systems with Microsoft patches and antivirus (AV) software, and have raised the importance of maintaining solid backups with well-documented recovery procedures. Each of these items must be addressed in contingency planning as attacks are becoming more prevalent and utilities

[5] Ken Palmer, "Lansing utility paid $25,000 ransom after cyberattack," Detroit Free Press, November 9, 2016, https://www.freep.com/story/news/local/michigan/2016/11/09/bwl-paid-ransom-cyberattack/93576218/.

[6] Scott Liles "City erases, re-installs server after ransomware attack." March 14, 2017. https://www.baxterbulletin.com/story/news/local/2017/03/14/city-erases-re-installs-server-after-ransomware-attack/99128740/.

[7] "European water utility attacked by cryptocurrency mining malware," Smart Energy International, February 13, 2018, https://www.metering.com/regional-news/europe-uk/cryptocurrency-malware-eu-utility/.

appear to be in the firing line of these advanced persistent threats.

## Challenges of Implementing Cybersecurity Initiatives in ICS

There are many challenges of implementing cybersecurity initiatives in an ICS environment. Technology plays an important role in controlling and monitoring ICS environments, but can be challenging in regards to vulnerabilities from cyberthreats. Many of the accepted practices, such as air gapping, are being challenged by new cyberthreats that have recently come to light and are not as foolproof as once was believed. We now compare the business network to a typical ICS SCADA network.

Basic Business Networks - Networks are made up of multiple devices, such as servers, computers, printers, and wireless access points that are connected to switches and routers. If you connect to the Internet at your home, you have a small network that works based on these same principles. On a typical business network, these devices communicate primarily using TCP/IP Ethernet technology, and in most cases are built on Microsoft using drivers and software that are tested thoroughly in the business environment.

Basic SCADA Networks - In contrast, an ICS or SCADA network interfaces to all of these devices as well as additional devices such as PLCs, operator interface terminals (OITs), flow/pressure meters, and closed-circuit television (CCTV). Some of these devices, especially PLCs, often communicate using variants of the TCP/IP protocols, and in some cases other bus-based protocols such as Modbus and Profibus. An ICS network also utilizes a mixture of operating systems and drivers – not just Microsoft – which adds to the complexity of supporting and updating an ICS network.

System Development Life Cycle - A typical control system is expected to last seven to ten years; but as time passes, your security protection diminishes. As warranties expire, support contracts end if not extended, and maintenance options decrease for new parts and software. This leads to vulnerabilities in systems at the end of this cycle signaling the need planning for a new system and getting hardware and software with more built-in cybersecurity features.

## Trends in Cybersecurity in Water/Wastewater

Let's explore recent trends in cybersecurity protection and response in the water/wastewater market.

*Process Improvements*

National Institute of Standards and Technologies (NIST) cybersecurity framework provides guidance and recommendations on how water/wastewater facilities can address cybersecurity needs. NIST, under the U.S. Department of Commerce, is directed in Executive Order 13636 to provide the standards and guidance for a Cybersecurity Framework for our nation's critical infrastructure. This Executive Order references the framework as voluntary and not mandatory with regards to the water sector.

Two specific NIST documents relevant to the water sector are NIST Special Publication (SP) 800-53 Revision 5 – "Security and

Privacy Controls for Federal Information Systems and Organizations" – and NIST SP 800-82 Revision 2 – "Guide to Industrial Control Systems (ICS) Security." NIST Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, is a massive document developed with the help of the Department of Defense (DOD), DHS, and other government entities; it provides guidance for federal information systems in regards to cybersecurity best practices. This addresses aspects of the SCADA network that incorporate the business network hardware and software. NIST SP 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security, provides guidance more specific to water/wastewater with its PLCs and other controls devices. NIST breaks down into 18 sections control families that can be designed to evaluate ICS for cybersecurity shortcomings using NIST publications 800-53 and 800-82. As part of this process, risks will be identified. As risks are identified, they are reported to management so that management decides whether to take steps to address the risk or to accept the risk. This process is continual, allowing the program to continuously monitor and identify risks that may not have been identified in previous audits, or to root out new threats as they come to light. Steps are defined for threat prevention and responding to cybersecurity threats, in addition to personnel roles for response and reporting.

Further guidance for our industry came in 2014 when the American Water Works Association (AWWA) created the Process Control System Security Guidance for the Water Sector, which provides step-by-step guidance for protecting water sector PCS (Process Control Systems) from cyberattacks. This document references a Cybersecurity Guidance Tool, which is accessed through a web interface in which the user checks a list of predefined cases that generates a prioritized list of recommendations based on specific needs of the water utility in question. This list references documents such as NIST SP 800-53 and SP 800-82, pointing out policies and procedures that can be applied to that specific water utility in its creation of a cybersecurity program. This program is free and can be found on AWWA's website (www.awwa.org).

*Technology Improvements*

Water utilities are making use of Segmentation of Networks, which breaks up networks into different subnets with strict access controls for devices connecting with each network. Also, the use of highly secure DMZ (Demilitarized Zone) networks allows the OT network to pass information into this intermediate network, which is then securely moved into the IT (business) network thus providing protection to the precious inner SCADA networks'.

Water utilities are making progress in areas of backing up of data and systems. With ransomware causing a panic, there is more emphasis for this activity. Acronis backup software provides a good starting point for a smaller utility because of its backup functionality and low-cost entry point.

Several utilities are successfully upgrading HMI application servers and historians to virtual machines using VMware and Microsoft Hyper-V. Virtualization helps with

disaster recovery, allowing VMs to be moved to similar virtual environments without having to configure the VM's drivers and configurations of software related to the SCADA environment before using.

Water utilities have made improvements in Defense in Depth strategies such as antivirus (AV), firewall protection, network monitoring utilities, and Intrusion Detection Systems (IDS) on the perimeter of SCADA networks by utilizing some of the new products that have been developed. Belden's Tofino firewalls is one example that offers deep packet inspection of network traffic and goes beyond what is usually offered in standard firewalls geared towards ICS networks. Another example is Rockwell Automation which leverages Cisco technology in Stratex switches for deep packet analysis capabilities.

*People Improvements*

Utilities in the water sector that have made progress in implementing cybersecurity initiatives have been characterized by a strong commitment to the cause from upper management. And from this, Information Technology (IT) and Operations Technology (OT) groups work closely together to blend skills and knowledge from both sides. Maintenance and Emergency Response groups also need to be included in this process.

OT personnel understand how ICS networks work and how the different protocols can affect their systems. Their skills will need to be leveraged in this process to continue to monitor and control successfully. IT doesn't have the same level of expertise in understanding PLC, HMI, and OIT or how they communicate; it is imperative that each group work together for successful implementation of new products and procedures.

In some cases, the IT group leverages what they are already doing on the business network with areas such as system and data backup, AV/firewalls on computers and servers, network monitoring, and port management on routers and switches. The future will hold more planned patching of Microsoft Critical Updates (MSCU) to SCADA PCs/Servers programs while understanding the importance of having test beds that will test if the patches/updates will break communications. IT will need to work closely with OT personnel as each layer of defense-in-depth is added.

Some of the bigger water utilities are doing stress testing in lab sandbox environments. With servers and PLC equipment configured exactly as in the field system, IT/OT personnel are able to test antivirus, intrusion detection systems (IDS), MSCU, and SCADA software upgrades/updates without fear of taking down a working system. Water utilities are finding it beneficial to conduct risky tasks such as penetration testing for vulnerabilities in lab environments without the risk of interrupting the ICS network performance.

Vendors of HMI systems, such as Wonderware and GE iFix, test their systems in lab environments with Microsoft Critical Updates to verify their systems can handle the new security patches, usually within a month or two of the patches being released.

But, at the other end of the spectrum, we have also come across water utilities groups

that have not made much progress and still need to develop an initial cybersecurity program. These utilities should start asking questions and make sure when talking to firms that they understand not only IT business networks, but also SCADA networks, as they seek these solutions.

Awareness and Training are an extremely important part of the NIST system. Some water utilities are using training videos such as KnowBe4 created by Kevin Mitnich, the famous ex-hacker, to provide CBT (Computer-Based Training) videos for their personnel.

The DHS ICS-CERT can perform audits of water utilities of ICS networks and systems. This process is helpful for utilities to begin to understand how vulnerable they truly are, and can help in getting future funding to make improvements in cybersecurity. But, some water utilities are hesitant to allow these audits to occur on their system, even if the service is free.

Water utilities are seeking cybersecurity personnel to improve their level of expertise in this area. But, finding the right people with the right skills is not always easy.

## Conclusion

Our drinking water is very important to us. Water utilities' ability to produce safe water in the quantities needed to support our communities is paramount for our society's ability to grow and thrive. Also, the public's trust of water utilities is very important to maintain as well. Cyberattacks pose a threat to water and wastewater utilities' ability to process water and threat wastewater. Because the dependency on technology to control utilities has increased year to year, using plant personnel to manually control water and wastewater utilities is not cost effective. ICS systems in the water sector have a long way to go before they catch up to the level of cybersecurity such as industries like electric utilities and the oil and gas industry. However, many water utilities are beginning to make improvements to cybersecurity in their networks due to the questions upper management and risk managers are asking on the subject. Many utilities are beginning to use NIST/AWWA frameworks to revamp their cybersecurity. This is a sign that they are moving in the right direction because the cyberthreats are not going to stop anytime soon.