INL/JOU-16-39302
Accepted Manuscript

PROTECTING DRINKING WATER UTILITIES FROM CYBER THREATS

Robert M. Clark, Srinivas Panguluri,
Trent D. Nelson, Richard P. Wyman

July 2016

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Prepared for the U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

PROTECTING DRINKING WATER UILITIES FROM CYBER THREATS

Robert M. Clark[1], Srinivas Panguluri[2], Trent D. Nelson[3], and Richard P. Wyman[4]

[1] Environmental and Public Health Consultant, 9627 Lansford Drive. Cincinnati, OH 45242, USA. Phone: 513-891-1640. E-mail: rmclark@fuse.net.

[2] CB&I Federal Services LLC, 5050 Section Avenue, Cincinnati, OH 45212, USA. Phone: 513-782-4893, E-mail: Srinivas.Panguluri@cbifederalservices.com.

[3] Cybersecurity Consultant, P.O. Box 3545, Idaho Falls. ID 83415, USA. Phone: 208-526-2512. E-mail: **Trent.Nelson@inl.gov**.

[4] Control Systems Engineer, P.O. Box 3545, Idaho Falls. ID 83415, USA. Phone: 208-526-1249. E-mail: **Richard.Wyman@inl.gov**.

ABSTRACT

Cyber-security challenges have the potential for becoming one of the defining issues of our time. Cyber-attacks have become an ever-increasing threat and the United States (US) Federal Bureau of Investigation (FBI) now ranks cyber-crime as one of its most important law enforcement activities. In addition to the general problems associated with cyber-crime, critical infrastructure (CI) related to energy production, manufacturing, water supply and other systems have come under attack. For example, drinking water utilities are increasingly incorporating computer technology into their routine operations and are therefore increasingly vulnerable to cyber-threats. Systems control and data acquisition (SCADA) systems used to manage automated physical processes essential to water treatment and distribution systems have become standard in medium to large drinking water utilities and in many small water systems. However, even with

the application of standard information technology cybersecurity best practices these types of systems have proven to be vulnerable to cyber-attacks. In 2015, the US Department of Homeland Security (DHS) responded to 25 cybersecurity incidents in the Water Sector and to 46 incidents in the Energy Sector. Comparatively, between 2014 and 2015, the reported number of Water Sector incidents actually increased by 78.6% (from 14 to 25). The DHS is in a collaborative partnership with the US Environmental Protection Agency to ensure cybersecurity in the Water Sector. As a result of this partnership a number of guidance documents and techniques have been developed to counter cyber-attacks and minimize cyber vulnerability. These approaches are documented along with a summary of common vulnerabilities. A new approach which has great promise in protecting drinking water systems against hacking and cyber-attacks, based on the concept of unidirectional gateways, is presented and discussed.

INTRODUCTION

Water supply professionals and government planners have long been aware that urban water systems are vulnerable to a number of manmade and natural disasters including water shortages and droughts, earthquakes, and storms (Clark and Hakim, 2016; Janke et al., 2014). After the attacks of September 11, 2001, government planners in the US have been forced to consider the vulnerability of all of the nation's critical infrastructure, including water systems, to terrorism. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (U.S. Congress, 2002) intensified this focus on water security. On December 17, 2003, Homeland Security Presidential Directive 7 (HSPD-7, 2003), established a national policy for Federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. It established the US Environmental Protection Agency (EPA) as the

lead agency for the Water Sector's critical infrastructure protection activities. Initially, the EPA focused on physical security however, with the rapid proliferation of computer systems and telecommunication networks cyber-security has become an area of increasing concern. Cyber-security is an increasing focus in the water industry because water utilities are increasingly using industrial control system (ICS) networks to control the physical processes essential to water treatment and distribution systems (Ginter, 2016). Drinking water utilities have become dependent on SCADA systems which are a class of ICSs that are becoming standard for all medium to large drinking water utilities. SCADA systems are frequently integrated into large-scale processes that can include multiple sites and large distances.

This paper will discuss the following:

- US concerns over cyber-security.
- Relationship of cyber-security to critical infrastructure protection.
- Designation of water supply in the US as critical infrastructure.
- New technological approaches that can be used to enhance protection of critical infrastructure including water supply systems.

CYBER-SECURITY CHALLENGES IN THE UNITED STATES

In 2009, the President of the US declared cyber threats to be among "the most serious economic and national security challenges we face as a nation" (Obama, 2009). It is clear that challenges related to cyber-security have the potential for becoming one of the defining issues of our time and according to President Obama "America's economic prosperity in the 21st century will depend on cyber-security" (Obama, 2009). In January 2012, the US Director of National

Intelligence in testimony before the House of Representatives stated that cyber threats pose a critical national and economic security concern (Clapper, 2012). A US Government Accountability Office (GAO) report issued in 2013 states that, cybersecurity threats to systems supporting critical infrastructure and federal information systems are evolving and growing in the US (US GAO, 2013).

Executive Order 13636 (Accessed on June, 2, 2016 from https://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical) was issued in February 2013, with the intent of improving the cyber security of US critical infrastructure (CI) (Fischer, et al. 2103). The order attempted to enhance the security and resiliency of US CI through voluntary, and collaborative efforts including:

- Expanding an existing Department of Homeland Security (DHS) program for information; sharing and collaboration between the government and the private sector.
- Developing a process for identifying CIs that have a high priority for protection.
- Requiring the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework of standards and best practices for protecting CI.
- Requiring regulatory agencies to determine the adequacy of current requirements and their authority to establish requirements to address the risks.

Commonly recognized cyber-aggressors include (Fischer, et al. 2013):

- Cyber-terrorists who are state-sponsored and non-state actors who engage in cyberattacks as a form of warfare.

- Cyber-spies stealing classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage.
- Cyber-thieves engaged in illegal cyberattacks for monetary gain.
- Cyber-warriors who are agents or quasi-agents of nation-states who develop capabilities and undertake cyberattacks in support of a country's strategic objectives.
- Cyber-hactivists who perform cyberattacks for pleasure, or for philosophical or other nonmonetary reasons.

Even though cyber-threats pose a major threat to CI, in the US, the Federal role in what is now called cyber-security has been debated for more than a decade. One of the reasons action at the Federal level for protecting CI is limited lies in the political structure of the US. In the US, State and local governments have been the major institutions responsible for providing services to their populations. In addition, the US Constitution provides for a separation of powers between the States and the Federal government. Therefore, the National Governors Association (NGA), a non-partisan organization representing the interests of the fifty states and trust territories, is taking action in this important area (Saparito, 2014).

According to the US GAO (2011) advanced persistent threats (APTs) pose increasing risks in the US and throughout the world. APTs occur where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives repeatedly over an extended period of time. These objectives may be perpetrated by foreign militaries or organized international crime. Growing and evolving threats can potentially affect all segments of society, including individuals, private businesses, government agencies, and other entities. Cyber-based attacks

can result in the loss of sensitive information and damage to economic and national security, the loss of privacy, identity theft, or the compromise of proprietary information or intellectual property. US Federal agencies have reported that in the period between 2006 and 2012, the number of cyber security incidents has increased dramatically. According to the U.S. Computer Emergency Readiness Team (US-CERT), over this period, these incidents have increased from 5,503 to 48,562; an increase of 782 percent (US GAO, 2013). The US FBI now ranks cybercrime as one of its most important law enforcement activities. President Obama's recently proposed budget would sharply increase annual spending on cybersecurity, from $13 to $14 billion (Accessed on March 7 2016 from http://www.techinsider.io/cyberattacks-2015-12 ; Accessed on March 7, 2016 from http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0).

WATER SYSTEM SECURITY IN THE US

Both from a public health and an economic perspective, water supply represents a critical infrastructure that must be protected. After September 11, 2001, the federal government directed efforts to secure the nation's critical infrastructure and initiated programs such as the National Strategy to Secure Cyberspace (Bush, 2003). This program addresses the vulnerabilities of SCADA systems a.k.a. ICSs and called for the public and private sectors to work together to foster trusted control systems. As has been discussed SCADA/ICS systems are an essential component for the effective operation of most water utilities in the U.S. Homeland Security Presidential Directive (HSPD–7, 2003) and its successor, the Presidential Policy Directive issued in 2013 (Accessed on June 2, 2016 from https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

reaffirmed the Water sector as one of the sixteen critical infrastructure sectors that must be protected.

In 2015, the DHS responded to 245 incidents reported by asset owners and industry partners as summarized in Figure 1. According to the data in Figure 1 the Water sector reported the fourth largest number of incidents resulting in DHS incident response support behind Critical Manufacturing, Energy, and Unknown (DHS 2016). As can be seen in the figure the second largest number or reported incidents was in the Energy sector which could have a direct impact on water supply systems.

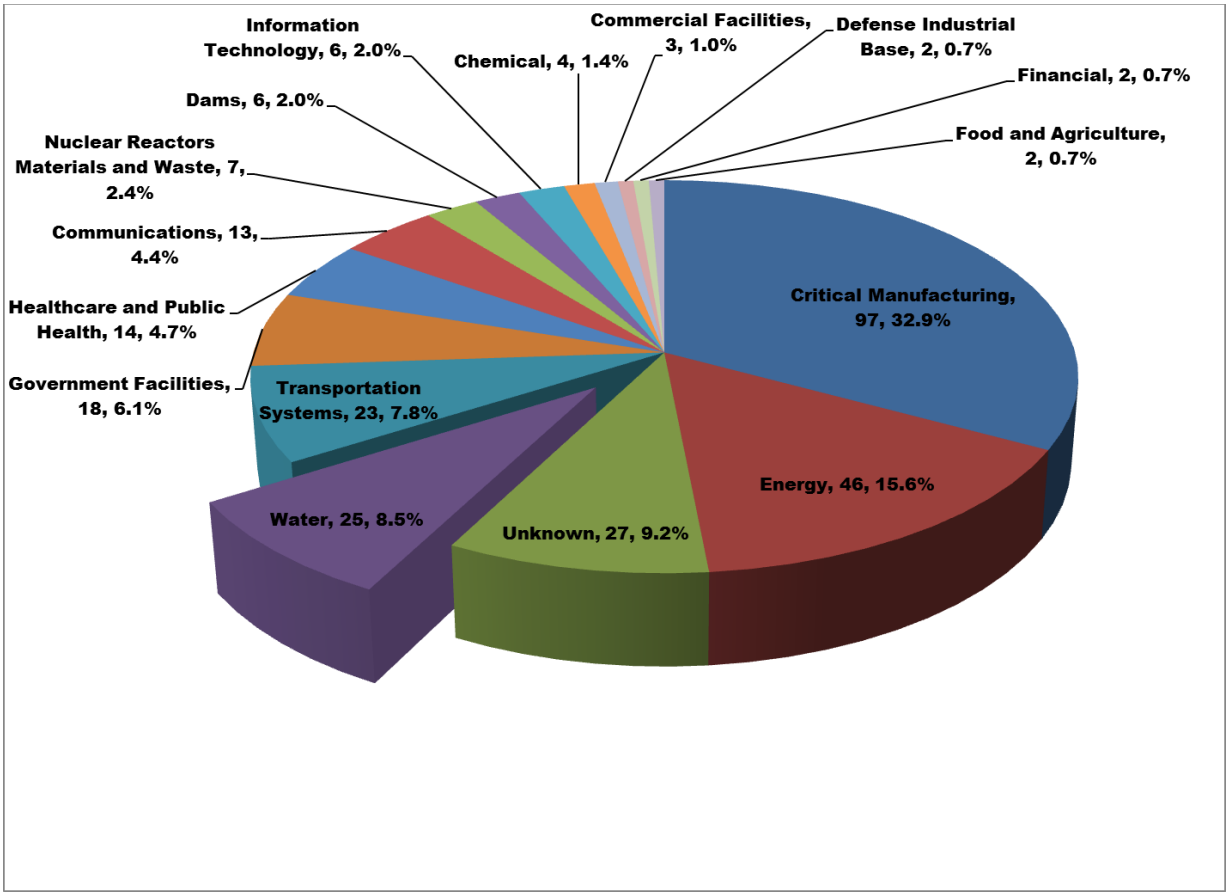

Figure 1. 2015 security incidents reported by sector (DHS, 2016)

While the EPA is the Sector-Specific Agency (SSA) lead for protecting the critical infrastructure in the Water Sector, it works collaboratively with the DHS, utility owners and operators, as well as representatives from industry associations. The goal is to ensure that Water Sector cyber-protection and resilience strategies are effective and practical.

To manage cybersecurity risks, EPA as the Water Sector lead, has undertaken a collaborative voluntary partnership model. Specifically, under section 10(a) EO 13636 (Accessed on June, 2, 2016 from https://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical). EPA has determined that current cybersecurity regulatory requirements in the Water Sector are sufficient and contemplates no regulatory action.

Public Water Systems

EPA classifies public water systems (PWSs) based on the number of people they serve: (1) very small water systems serve 25–500 people, (2) small water systems serve 501–3,300 people, (3) medium water systems serve 3,301–10,000 people, (4) large water systems serve 10,001–100,000 people, and (5) very large water systems serve more than 100,001 people. Figure 2 shows the estimated distribution of the PWSs in these size categories and population served as reported by the EPA (US EPA, 2011; Panguluri et al., 2014).

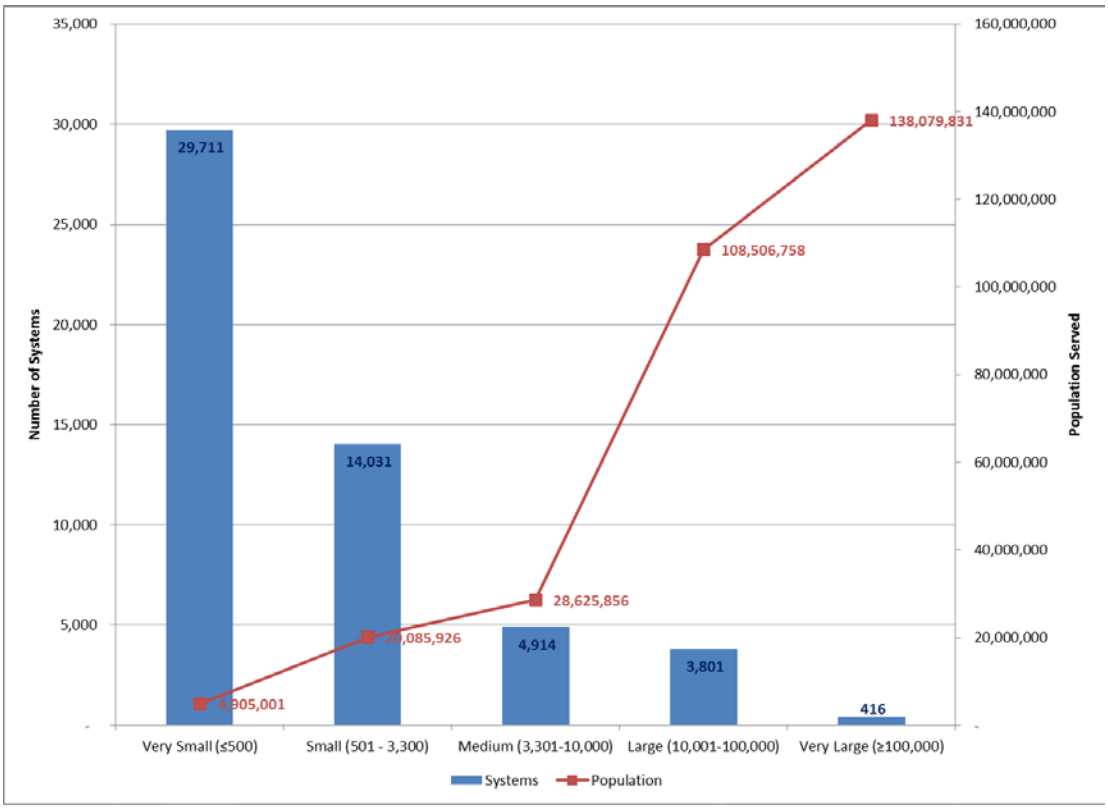

Figure 2 Distribution of the PWSs by system size and population served (US EPA, 2011).

The majority of drinking water systems in the US are small and very small. This figure represents only the community water systems in the U.S. A community water system is defined by EPA to include PWSs that supply water to the same population year-round. Therefore these statistics exclude the transient/non-transient non-community water systems which will more than quadruple the number of very small systems (from 29,711 to 131,073) and bring the total closer to the 155,000 drinking water systems in the U.S. as reported by EPA. Overall, it is estimated that the cost of producing a thousand gallons of water (or 3,785 liters) in the US can range between $3.37 for a very large PWS and $5.37 for a very small public PWSs (Panguluri et al., 2014).

Cybersecurity Initiatives

Sector-specific partners include: the EPA, DHS, the NIST, the American Water Works Association (AWWA), the Water Research Foundation (WRF), the Water Environment Research Foundation (WERF), other water associations, educational institutions, national research laboratories, public and private research foundations, states/local agencies, PWSs, and related organizations. Some of the collaborative cyber initiatives are discussed in the following paragraphs.

National Institute of Standards and Technology

NIST recently issued a document entitled, "Framework for Improving Critical Infrastructure Cybersecurity" (NIST, 2014). The cybersecurity framework presented in this paper is based on the NIST framework.

US Department of Homeland Security

The DHS has established the Critical-Infrastructure Cyber Community (C3) Voluntary Program as a partnership to increase awareness and use of the NIST Cybersecurity Framework. The C3 Voluntary Program is designed to connect Water Sector participants with DHS and other federal government programs to provide resources that will assist their efforts in managing their cyber risks. The DHS's US-CERT leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans.

American Water Works Association

In an effort to provide PWSs with more actionable information on cybersecurity, AWWA has released the Process Control System Security Guidance for the Water Sector (AWWA, 2014) and a supporting Use-Case Tool. The goal of the AWWA guidance is to provide water sector utility owners/operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyber-attacks as recommended by the American National Standards Institute (ANSI)/AWWA G430 and the EO 13636 (Accessed on June 2, 2016 from https://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical).

The ANSI/AWWA G430 (AWWA, 2015) standard defines the minimum requirements for a protective security program for the Water Sector. It is designed to promote the protection of employee safety, public health, public safety, and public confidence. This standard is one of several in AWWA Utility Management series designed to cover the principal activities of a typical PWS. This AWWA standard has received the SAFETY Act designation from the DHS in February 2012.

The G430 standard is intended for all PWSs regardless of size, location, ownership, or regulatory status. This standard builds on the long-standing Water Sector practice of utilizing a "multiple barrier approach" for the protection of public health and safety. The requirements of this standard are designed to support a protective utility-specific security program and are expected to result in consistent and measurable outcome. They address the full spectrum of risk

management from organizational commitment, physical and cyber security, and emergency preparedness.

US Environmental Protection Agency

As the Water Sector lead agency, the EPA encourages PWSs to use the NIST Cybersecurity Framework and participate in the DHS Voluntary C3 Program. The voluntary cybersecurity framework provides a flexible performance-based and cost-effective approach to help PWSs assess and manage cyber risk. The selected approach must also include provisions to protect business confidentiality, individual privacy and civil liberties (Stoner, 2014).

Cybersecurity Risk

Cyber-attack is one risk that all utilities share unless they are a very small utility that does not use computers to monitor and control its processes or manage its business. However, even these organizations are not immune from the impacts of a successful cyber-attack against a supporting service provider like the electric utility. Given that cyber-attacks against the water sector are a growing problem, managers must learn to manage cyber risk just like they manage other risks.

Advanced Persistent Threats

In an increasingly connected world, threats can originate from anywhere and be executed by anyone, but, as mentioned previously, APTs are usually the most dangerous. They are typically organized groups such as rival nation-states or terrorists that are highly committed and have vast resources to harm critical infrastructure targets.

Of the total number of incidents reported to ICS-CERT in 2014, roughly 55 percent involved APTs or sophisticated actors. Other actor types included hacktivists, insider threats, and criminals. APT pick specific targets and goals, depending upon their objectives. Their objectives may include exfiltrating data, sabotage, and/or shut down the process. In order to conduct any one of the goals, the APTs need to know the following specific information to accomplish their goals:

- Detailed design information of the control system and/or the process.
- Access to the facility (electronically and/or physically).
- Understanding of the system(s) and process.
- Knowledge of weaknesses and vulnerabilities that can be exploited to gain the required access.

Common Vulnerabilities in the Water Supply Industry

Historically, business and SCADA networks were separate because the network topologies were vastly different. Even if a utility owner recognized the value of integrating SCADA data into their strategic decision support systems, limitations in network topologies made integration difficult. Older SCADA systems relied heavily on serial connectivity and very low frequency radio communications that could provide enhanced range and partial line-of-sight connectivity, none of which supported standard internet protocol (IP) connectivity desired by business networks (Panguluri et al. 2011). This virtual isolation has led to a false sense of security by many SCADA system administrators. Increasingly, however, SCADA and business networks of most medium- to large-scale PWSs are inter-connected to provide more integrated operation. If such integration is not secured properly, it will generally lead to greater vulnerability and the

water sector is generally believed to lag most other critical infrastructures in securing their control systems (Baker et al., 2010; Weiss, 2014). The top five areas of common security gaps in water supply are: 1) network configurations, 2) media protection, 3) remote access, 4) documented policies and procedures, and 5) trained staff.

Consequences of cyber attacks

Based on a hacker's motivation and objectives, he (or she) may try to extract information (data) to further develop attacks or sell the information for gain. With PWSs if the objective is to cause public distrust or fear, the hacker may attempt to discharge contaminated water, deny access to the system, and/or destroy equipment. Most all hackers will also change files to cover their tracks to be undetectable. Cyber-impacts may also have process impacts and may vary depending on the process and how the system is designed. For instance in a PWS, if an attacker changes database parameters in the real-time database (impacts system integrity) they could turn on pumps causing a tank to overflow. An often cited example of a successful attack against a wastewater treatment plant occurred in the Maroochy Shire in Queensland, Australia (Panguluri et al. 2004; Weiss 2014). The attack resulted in raw sewage spill into rivers, parks and the grounds of a nearby hotel. The main consequence in this case, was environmental damage and societal costs.

The attack was conducted by a former insider Vitek Boden. Mr. Boden formerly worked for Hunter Watertech, an Australian firm that originally installed the SCADA radio-controlled sewage equipment for the Maroochy Shire Council. Between February 28, 2000 and April 23, 2000, Mr. Boden issued radio commands to the sewage equipment on 46 separate occasions that

resulted in spills. During this period, the sewerage system experienced the following series of faults (Weiss, 2014):

- Pumps were not running when they should have been.
- Alarms were not reporting to the central computer.
- A loss of communication between the central computer and various pumping stations.

Another employee of Hunter Watertech was appointed to review the aforementioned series of faults. He began monitoring and recording all signals, messages, and traffic on the radio network. As a result of his investigations, he (along with other experts) concluded that many of the problems were the result of human intervention rather than equipment failure. Additionally, the faults associated with the attack ceased after Mr. Boden was arrested.

PROTECTING DRINKING WATER SYSTEMS

Creating a Cybersecurity Culture

Most water managers are unfamiliar with information technology (IT) and ICS/SCADA technology, much less cyber security defenses, and must depend on their technical staff, however, there are steps that managers can take to secure their systems against cyber-attacks. There are several publications, as previously discussed, that can provide useful guidance on this area (Panguluri, et al., 2016)). Fisher (2014) lists an eight-stage process for creating major change:

- Establishing a sense of urgency – Identify and discuss the crises or potential crises.
- Creating the guiding coalition – Putting together a group with the power to lead change.

- Developing a vision and strategy including policies and procedures to define and enforce security.
- Communicating the change vision.
- Empowering broad-based action.
- Generating short-term wins.
- Consolidating gains and producing more change.
- Anchoring new approaches in the emergent culture.

Establishing a cyber-security culture is the framework for implementing a strong defense in depth program. It puts the three legs (technology, people, and physical protection) of cyber-security on a firm foundation. Physical protection implies locating IT equipment in a safe location.

Secured Network Design

It has been traditional for industrial control systems to apply standard, IT security systems to control networks, including physical security, personnel security, and ICS network perimeter protections including firewalls and network intrusion detection systems (NIDS). However, a Ponemon Institute study (Ponemon, 2013) found that malicious cyber breaches took an average of 80 days to detect, and 123 days to resolve. Therefore, experts are recommending technological innovations such as unidirectional gateways be used as the modern alternative to firewall perimeter protections for ICSs. An example of a unidirectional gateway deployment is illustrated in Figure 3. All unidirectional gateways are combinations of hardware and software as shown below. A unidirectional gateway results in a system able to transmit information from a protected individual network, but physically unable to transmit any information back to that

protected network from outside the system. This could be considered the optimal security approach.

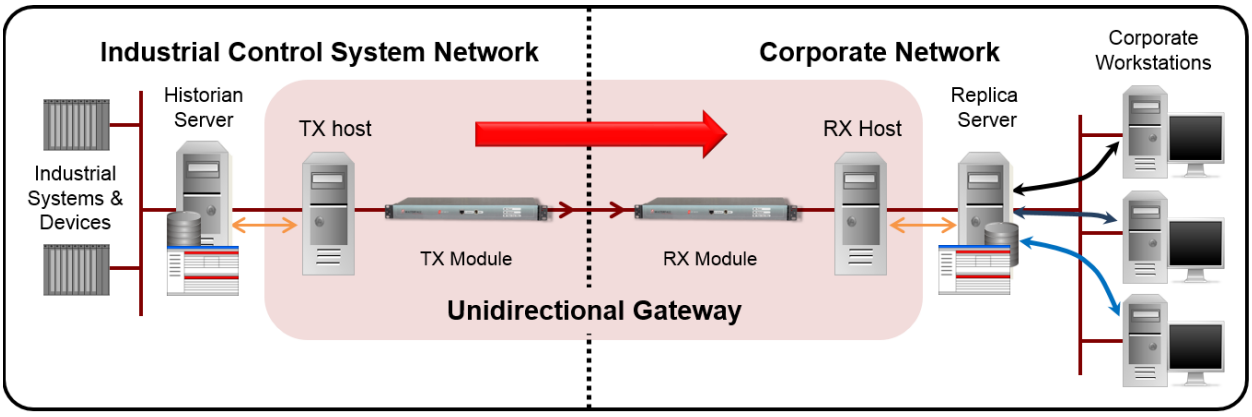

Figure 3. Example of a Unidirectional Network (Ginter, 2016)

In cases where a unidirectional gateway is unaffordable (e.g., the smaller-sized utilities) or technically challenging to implement, one should investigate other alternatives such as implementing virtual routing and forwarding (VRF). VRF technology is included with some off-the-shelf routers that allow for multiple instances of a routing table to exist in a router and work simultaneously. This allows for network paths to be virtually segmented without using multiple devices. Internet service providers often take advantage of VRF functionality to create separate virtual private networks (VPNs) for customers. This technology is also referred to as VPN routing and forwarding.

Good cybersecurity designs strive to limit access or incorporate isolation capabilities of ICS/SCADA systems. The isolation of a ICS system can be achieved by establishing security enclaves (or zones) with virtual local area networks (VLANs) or subnets that are segregated from

lower security zones like corporate networks or any Internet accessible zones. Information passing from one security zone to another should be monitored. Figure 4 illustrates an example of a secure PWS architecture.

In this example the ICS environment has been isolated with no ingress electronic connections. The use of data diodes between the SCADA/ICS and corporate information technology (IT) environments allows for information sharing from the ICS environment through a truly one-way transfer of data from ICS historians (databases) for business needs and reporting. The use of true isolation through data-diode technologies between the treatment plant ICS and the corporate environment (Figure 4) is more recent. The adoption of this technology within the water sector has been observed by the authors at one utility but is gaining increasing acceptance within the water sector. Some PWSs have identified the use of this technology in their advance security posture planning documents. However the implementation of this technology requires an investment in both capital and manpower. At least two full-time-equivalent (FTE) technology staff are required for several months during the development, testing, verification and deployment phases. Additionally, depending upon the complexity of the architecture, a successful deployment may require three or more FTEs. After the full implementation and optimization of the secure PWS architecture, it is estimated that at least ¼ to ½ FTE will be necessary to manage and support this type of security posture. Based on current water sector cybersecurity implementation and execution costs, it is estimated that this

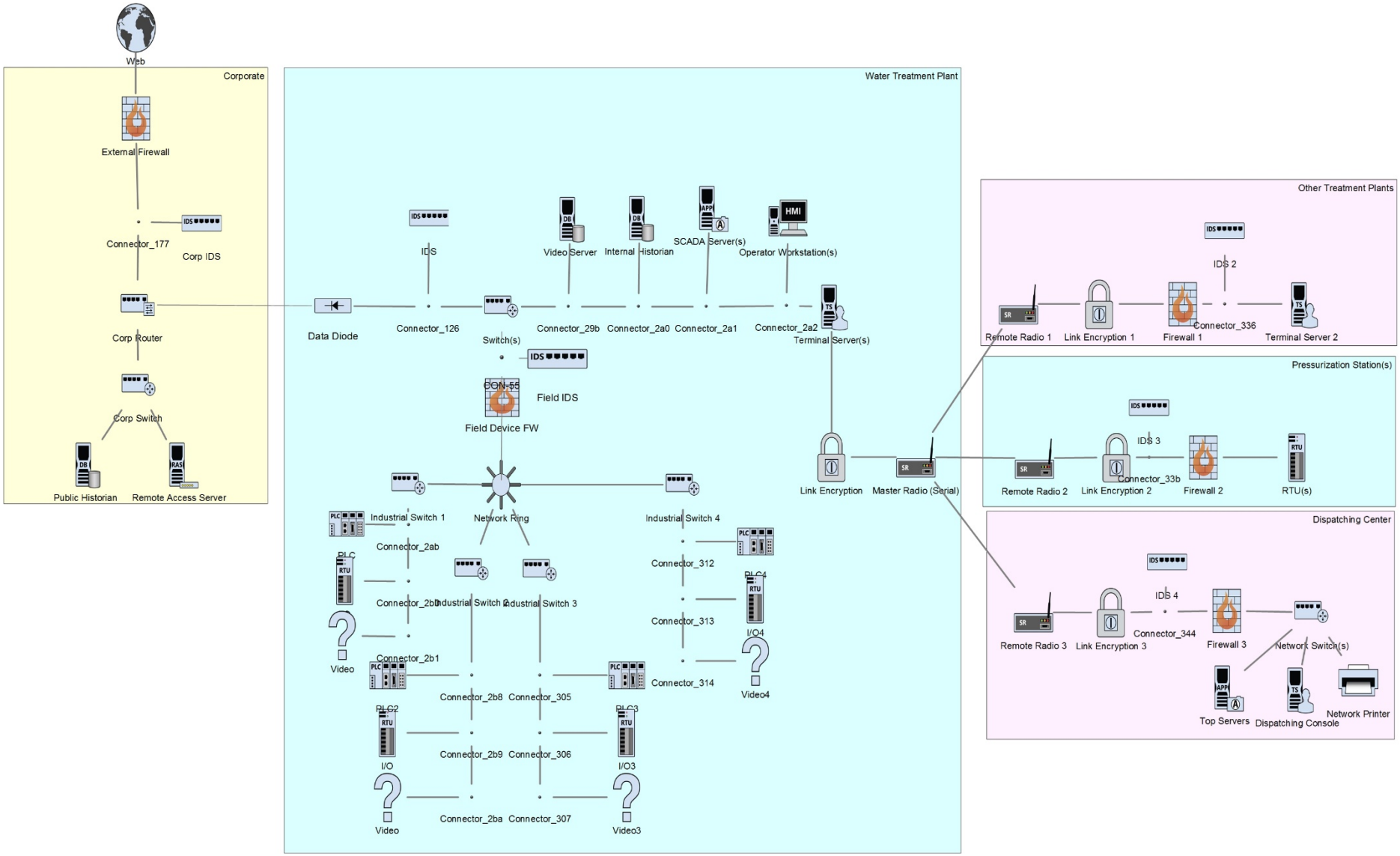

Figure 4. Secure PWS Architecture Example (Panguluri et al, 2016).

type of technology implementation (depending on the features) would average around $300,000 for initial implementation and optimization.

The application of secure architecture and isolation of the ICS environment prevents remote access connection and prevents unauthorized computers or network devices including 3rd party vendors from entering into the ICS environment. Furthermore, the utility will also need to address the issue of securely installing patches, anti-virus signature files and application updates. These approaches typically involve the use of portable media (USB memory and USB hard drives) which also present security concerns. By deploying Diode technology, the ~~threat~~ cyber risk of compromise ~~vector~~ from external networks, like the internet is significantly reduced if not eliminated. However, ~~will be reduced to insider threats and media protection~~trusted insiders, portable media, and physical intrusions still present a potential vector into the system. Therefore a strong media protection policy, as well as strong physical controls needs to be developed to maintain the integrity of the environment. Prior to adding a network device or computer to the ICS environment, a thorough analysis should be conducted and then the equipment reviewed and approved for use. Once approved, the equipment should stay at a secure off-site location for future use and identified as an ICS component.

The suggested architecture along with strong policies and procedures is necessary in order to develop a security culture and to raise the level of awareness of each employee. Management should provide support for training of the core cybersecurity staff for cybersecurity skills enhancements and development. The next stage in security is to monitor and verify that the security controls are working as designed through monitoring and log-file analysis. Systems,

applications and security components should enable logging. This capability should be centrally located through a security information and event management (SIEM) system to allow central management of monitoring appliances. It should include log-reviews and alerting capabilities in the event that the system starts to identify anomalies with the systems for early detection, alerting and recovery capabilities.

These types of measures will result in a strong security design. Finally, when excessing or decommissioning equipment, a proper equipment disposal process should be in place to ensure no proprietary information ever leaves the environment. A proper disposal process protects from malicious reverse engineering, discovery, and reconnaissance activities.

SUMMARY AND CONCLUSIONS

The issue of cyber-security is currently having and will continue to have an impact on organized society throughout the world. In addition, as infrastructure becomes increasingly connected and capable of communicating, cyber-physical security in critical infrastructure such as water supply will become a major problem. In the US, cyber-security issues have become extremely important from a national security perspective (US GAO. 2013). However, in the US a strong desire for the separation of powers between the Federal government and the individual States has made developing a unified cyber-security strategy very difficult.

It is clear that cyber threats to the water sector are real. The insider attack on the Maroochy Shire wastewater treatment plant provides an insight into the real consequences of a specific attack and there have been confirmed cases of cyber-attacks against domestic water utilities.

Such an attack could impact public health and cause distrust of government officials, for example by delivering contaminated water that could potentially cause sickness (etc.) without detection.

In the US virtually all drinking water utilities, even subdivision sized systems, have become dependent on SCADA systems. Based on reports complied by the DHS the number of attacks in the water sector have increased between 2014 and 2015. It is therefore imperative that PWSs adopt suitable countermeasures to prevent or minimize the consequences of cyber-attacks. Establishing a strong cyber-security environment is the basis for implementing a strong in-depth cyber-defense. Such a program should consist of three legs (technology, people and physical protection). In this sense we are using physical protection as a surrogate for protecting cyber-devices from physical tampering. It is also critical that utility management must create a cyber security culture and provide management support. The lack of policies and procedures may be one of the great barriers to developing an adequate cyber-security – which would be driven by management support. If management support is lacking, then there will never be an effective cyber-security culture. A part of this philosophy is the concept of monitoring (SIEM) to verify security and the identification of potential issues, should be implemented.

Utilities should also avail themselves of the free opportunities available through DHS to train their staff and allocate necessary funding to achieve improvements in cybersecurity. The greatest challenge for the water industry is the large variance in system size, staffing, and resources available to the individual utilities. Utilities should adopt countermeasures that best meet their security and organizational requirements. Firewalls which are essentially devices ~~systems.~~ are important, but there is a growing application of unidirectional gateways which provide "hardware" solutions to protect critical infrastructure. Unidirectional gateways may be

the best security approach, but might not be practical for small to very small utilities due to the cost of the appliances. However, other options should also be discussed, which can also provide very good security posture include VRF and other technologies. The authors believe that no matter what approach utilities select they must utilize their resources to create a culture that prepares and then implements programs, including hardware that is designed to improve cybersecurity.

ACRONYMS

AD – active directory

ANSI – American National Standards Institute

APT - advanced persistent threats

AWWA - American Water Works Association

C3 - critical infrastructure cyber community

CI - critical infrastructure

DHS - Department of Homeland Security

EPA - Environmental Protection Agency

FBI - Federal Bureau of Investigation

FTE – full-time-equivalent

GAO - Government Accountability Office

ICS - industrial control systems

IP – Internet Protocol

IT – information technology

NIDS - Signature-based network intrusion detection

NIST - National Institute of Science and Technology

NGA – National Governors Association

OS – operating system

PWS - public water system

SCADA - supervisory control and data acquisition

SIEM - Security information and event management

SSA – sector specific agency

US - United States

USB – Universal Serial Bus

US CERT - US Computer Emergency Readiness Team

VLANs – virtual local area networks

VPN - Virtual private networks

VRF - Virtual routing and forwarding

WERF – Water Environment Research Foundation

WRF – Water Research Foundation

REFERENCES

Accessed on March 7, 2016 from http://www.techinsider.io/cyberattacks-2015-12

Accessed on March 7, 2016 from

http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0

Accessed on June, 2, 2016 from https://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical

Accessed on June 2, 2016 from https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

American Water Works Association (AWWA). 2014. Process Control System Security Guidance for the Water Sector. AWWA Government Affairs Office, 1300 Eye St. NW, Suite 701W, Washington, DC 20005.

American Water Works Association (AWWA). (2015). Security Practices for Operation and Management. AWWA Denver CO. 6666 W Quincy Ave, Denver, CO 80235

Baker, S., Waterman, S., and Ivanov, G. (2010). In the Crossfire – Critical Infrastructure in the Age of Cyber War. A global report on the threats facing key industries. McAfee International Ltd, 100 New Bridge Street, London EC4V 6JA, UK.

Bush, G.W.(2003). National Strategy to Secure Cyberspace. The White House, Washington, February, 2003.

Clark, Robert M., and Hakim, Simon. (2016). "Protecting Critical Infrastructure at the State Provincial and Local Level: Issues in Cyber-Physical Security" in Cyber-Physical Security at

the State, Provincial, and Local Level: Protecting Critical Infrastructure edited by Robert M. Clark and Simon Hakim. Springer International Publishers, Switzerland

Clapper, James R. (2012).Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence" January 31, 2012.

Department of Homeland Security (DHS). (2016). NCCIC/ICS-CERT Year in Review. National Cybersecurity and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team FY 2015. Issued by DHS's National Cybersecurity and Communications Integration Center. Available at: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf (Accessed on 6/18/2016)

Fischer, E. A., Liu, E. C., Rollins, J. and Theohary, C. A. (2013). "The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress." March 1, 2013, Congressional Research Service, 7-5700, www.crs.gov.

Fisher R. (2014). Applying Culture Change in Cyber Security to Enhance Homeland Security. Colorado Technical University Doctoral Symposium, October 16, 2014.

Ginter, A.P. (2016). “Cyber Perimeters for Critical Infrastructures” in Cyber-Physical Security at the State, Provincial, and Local Level: Protecting Critical Infrastructure edited by Robert M. Clark and Simon Hakim. Springer International Publishers, Switzerland

Homeland Security Presidential Directive 7 (HSPD–7).2002. Directive on Critical Infrastructure Identification, Prioritization, and Protection, Issued by the White House, December 17, 2003.

Janke, Robert, Tryby, Michael E. and Clark, Robert M. (2014). “Protecting Water Supply Critical Infrastructure: An Overview” in Securing Water and Wastewater Systems: Global Experiences edited by Robert M. Clark and Simon Hakim, Springer International Publishers, Switzerland. 2014.

National Institute of Standards and Technology (NIST). (2014). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014. Available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (Accessed on 3/28/2015)

Obama, Barrack. (2009).“Remarks by the President on Securing Our Nation’s Cyber Infrastructure” Washington, D.C., May 29, 2009)

Panguluri S., Haji S., Adams J., and Patel A. (2014). Drinking Water Purity – A Market Outlook. In: Ahuja S. (ed.) Comprehensive Water Quality and Purification, vol. 2, pp. 1-18. United States of America: Elsevier.

Panguluri, S., Nelson, Trent D., Wyman, Richard P. (2016). "Creating a Cybersecurity Culture for your Water/Waste Water Utility" in the State, Provincial, and Local Level: Protecting Critical Infrastructure edited by Robert M. Clark and Simon Hakim. Springer International Publishers, Switzerland

Panguluri S., Phillips, Jr. W.R., Ellis P. (2011). Cyber security: protecting water and wastewater infrastructure. In: Clark R.M., Hakim S., Ostfeld A. (eds.) Handbook of water and wastewater systems protection. Springer-Science, New York, pp 285–318

Panguluri S., Phillips, Jr. W.R., Clark R.M. (2004). Cyber Threats and IT/SCADA System Vulnerability. In: Mays L.W. (ed.) Water supply systems security. McGraw-Hill, New York. pp 5.1–5.18

Ponemon Institute LLC. (2013). The Post Breach Boom, Waterfall Security Solutions (2011) Introduction to Waterfall Unidirectional Security Gateways: True Unidirectionality, True Security

Saporito, Laura. (2104) "The Cybersecurity Workforce: States' Needs and Opportunities, Washington DC,; National Governors Association Center for Best Practices, October 27, 2014

Stoner, N., 2014. Reducing Cybersecurity Risks in the Water Sector: A Voluntary Partnership Approach. Blog dated February 12, 2014. Available at: http://blog.epa.gov/epaconnect/2014/02/reducing-cybersecurity-risks-in-the-water-sector-a-voluntary-partnership-approach/ (Accessed on 3/28/2015)

U.S. Congress. (2002). Pub. L. No. 107-305 (Nov. 27, 2002); 15 U.S.C.§ 7406(c)

US Environmental Protection Agency. (2011). Fiscal year 2010 drinking water and ground water statistics. EPA Office of Ground Water and Drinking Water. EPA 817K11001, June 2011.

United States Government Accountability Office (GAO). (2011). High Risk Series: An Update, GAO-11-278 (Washington, D.C.: February 2011).

United States Government Accountability Office (US GAO), (2013). CYBERSECURITY National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. GAO-13-187, February 2013

Weiss, J. (2014). Industrial Control System (ICS) Cyber Security for Water and Wastewater Systems, Clark R. M. and Hakim S. (eds.), Securing Water and Wastewater Systems, Protecting Critical Infrastructure 2, DOI: 10.1007/978-3-319-01092-2_3, Springer International Publishing, Switzerland.