Front. Earth Sci. 2011, 5(4): 406–413
DOI 10.1007/s11707-011-0199-5

RESEARCH ARTICLE

Protecting water and wastewater infrastructure from cyber attacks

Srinivas Panguluri (✉)[1], William Phillips[2], John Cusimano[3]

1 Shaw Environmental & Infrastructure, Inc., Cincinnati, OH 45212, USA
2 CH2MHILL, Gainesville, FL 32608, USA
3 Exida, Sellersville, PA 18960, USA

© Higher Education Press and Springer-Verlag Berlin Heidelberg 2011

Abstract Multiple organizations over the years have collected and analyzed data on cyber attacks and they all agree on one conclusion: cyber attacks are real and can cause significant damages. This paper presents some recent statistics on cyber attacks and resulting damages. Water and wastewater utilities must adopt countermeasures to prevent or minimize the damage in case of such attacks.

Many unique challenges are faced by the water and wastewater industry while selecting and implementing security countermeasures; the key challenges are: 1) the increasing interconnection of their business and control system networks, 2) large variation of proprietary industrial control equipment utilized, 3) multitude of cross-sector cyber-security standards, and 4) the differences in the equipment vendor's approaches to meet these security standards. The utilities can meet these challenges by voluntarily selecting and adopting security standards, conducting a gap analysis, performing vulnerability/risk analysis, and undertaking countermeasures that best meets their security and organizational requirements.

Utilities should optimally utilize their limited resources to prepare and implement necessary programs that are designed to increase cyber-security over the years. Implementing cyber security does not necessarily have to be expensive, substantial improvements can be accomplished through policy, procedure, training and awareness. Utilities can also get creative and allocate more funding through annual budgets and reduce dependence upon capital improvement programs to achieve improvements in cyber-security.

Keywords wastewater infrastructure, protecting water, cyber attacks

Received September 1, 2011; accepted September 27, 2011

E-mail: srinivas.panguluri@shawgrp.com

1 Background

Water supply infrastructure provides water to agriculture, industry (including various manufacturing processes, power generation, and cooling), business, firefighting, and our homes. Wastewater infrastructure is integral to the water supply infrastructure as it collects and treats wastewater prior to its discharge back to source water streams or lakes to complete the cycle. In the US, the President's Commission on Critical Infrastructure Protection report titled *Critical Foundations* (PCCIP, 1997) identified the water supply infrastructure as one of the critical infrastructures and was also the first US report to take a critical look at the vulnerabilities. Although the authors of this report found no evidence of an impending "cyber attack" on water supply infrastructure, they found widespread cyber-capability to exploit infrastructure vulnerabilities. Also, in 1997, a highly classified internal exercise code named "Eligible Receiver" was initiated by the US Department of Defense (DoD) in which a "red team" of hackers from the National Security Agency (NSA) was organized to infiltrate the Pentagon systems. The NSA team was only allowed to use publicly available computer equipment and hacking software. Although many details about Eligible Receiver are still classified, it is known that the red team was able to infiltrate and take control of the Pacific command center computers, as well as power grids, and 911 systems in nine major US cities (PBS, 2004).

The proliferation of information technology (IT) for organizational efficiency and the increased use of automated monitoring and control systems such as Supervisory Control and Data Acquisition (SCADA) systems for operational efficiency by the water and wastewater utilities operating this infrastructure have created cyber vulnerabilities that need to be appropriately addressed. The most recent high-profile targeted attack on a SCADA system was the Stuxnet worm attack. The Stuxnet computer worm

was discovered around June 2010, it was reported to have targeted Iranian nuclear facilities that were widely suspected to be uranium enrichment centers in Iran. An often cited water wastewater infrastructure-specific attack occurred at the Maroochy Shire Sewage Collection and Treatment System in Queensland, Australia. This attack occurred between February 9 th, 2000, and April 23rd, 2000, and resulted in the spillage of approximately 212000 gallons of raw sewage to nearby receiving water bodies. This attack was perpetrated by a disgruntled former insider, Mr. Vitek Boden, who on at least 46 occasions during the attack period issued unauthorized radio-commands to the SCADA system which resulted in the spill (Abrams and Weiss, 2008).

2 Water and wastewater cyber infrastructure overview

To defend water and wastewater infrastructure from a cyber attack, it is important to gain an overview and understanding of a typical utility's cyber infrastructure. The commonly used cyber-infrastructure terms are defined herewith:

- IT Infrastructure — interconnects and controls the flow of information across computer networks. IT infrastructure includes network routers, switches, gateways, wireless access points, radios, public communications networks and all types of cable media. IT infrastructure does not include the servers and computers that it interconnects. IT infrastructure can be limited to a single Local Area Network (LAN) serving a single networked application such as SCADA, or it can encompass a Metropolitan Area Network (MAN) spanning a Metropolitan Area and serving an entire municipality or all utility networked applications including SCADA, or it can encompass a Wide Area Network (WAN) spanning a larger geographic area such as those used by large corporations with offices located in multiple cities.
- Business Network — is the collection of interconnected devices designed to communicate and share data related to common business activities, such as administration of personnel and accounting. Depending on organizational characteristics, this network can reside totally within the water/wastewater utility or be split between the utility and some other governing body such as a District or City IT department.
- SCADA Network — consists of interconnected process monitoring and control devices and computers that collect, monitor, and adjust process control equipment using a LAN, MAN or a WAN and both wired and/or wireless media for communications. SCADA networks allow operators to monitor and control process units from a central and/or remote location. Also, recent trends indicate that the SCADA networks are often connected to the business network.

3 Infrastructure connectivity and safeguards

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, they couldn't because of limitation in the network topologies. SCADA systems relied heavily on serial connectivity and very low data-rate radio communications that could provide enhanced range and wireless connectivity, none of which supported standard IP connectivity desired by business networks. This situation led to "virtual isolation" of the SCADA network. This virtual isolation can lead to a false sense of security by many SCADA system administrators because they believed that these systems were unconnected to the outside world and thus could not be "hacked" into.

Increasingly the business case for integrating IT and SCADA systems is becoming hard to ignore. The benefits of SCADA/IT integration include (Panguluri et al. 2011):

- Shared Infrastructure — Business and SCADA systems in some cases, share MAN or WAN infrastructure to reduce the overall costs for leased or private lines. Proper segmentation of traffic will avoid the potential for security breaches.
- Shared Expertise — Common architecture components such as network, database and security can be managed by trained experts.
- Cheaper Components — SCADA systems can use cheaper transmission control protocol/internet protocol (TCP/IP) based components.
- Strategic Information Gains — SCADA data can be combined with data from other data sources such as laboratory information management system and geographic information system (LIMS/GIS) databases to produce or enhance real-time water quality modeling, forecasting capability, management/regulatory reporting, as well as providing utility facility status information for use by Emergency Response Centers during emergencies.
- Improved Overall Security Integration — Integration of physical security elements such as video monitoring with SCADA allows for 24/7 monitoring by SCADA operators.

These benefits are becoming hard to ignore and now there is a general push in the industry to eliminate the "islands of automation." Figure 1 shows a typical medium-to-large municipal government owned water and wastewater utility's IT infrastructure with interconnected SCADA and business networks.

Figure 1 represents a water and wastewater utility that operates two plants where the business and SCADA networks are connected by routers. The utility's cyber-infrastructure includes the following:

- A Local Exchange Carrier (LEC) managed wire-line MAN connecting plants to the municipal government

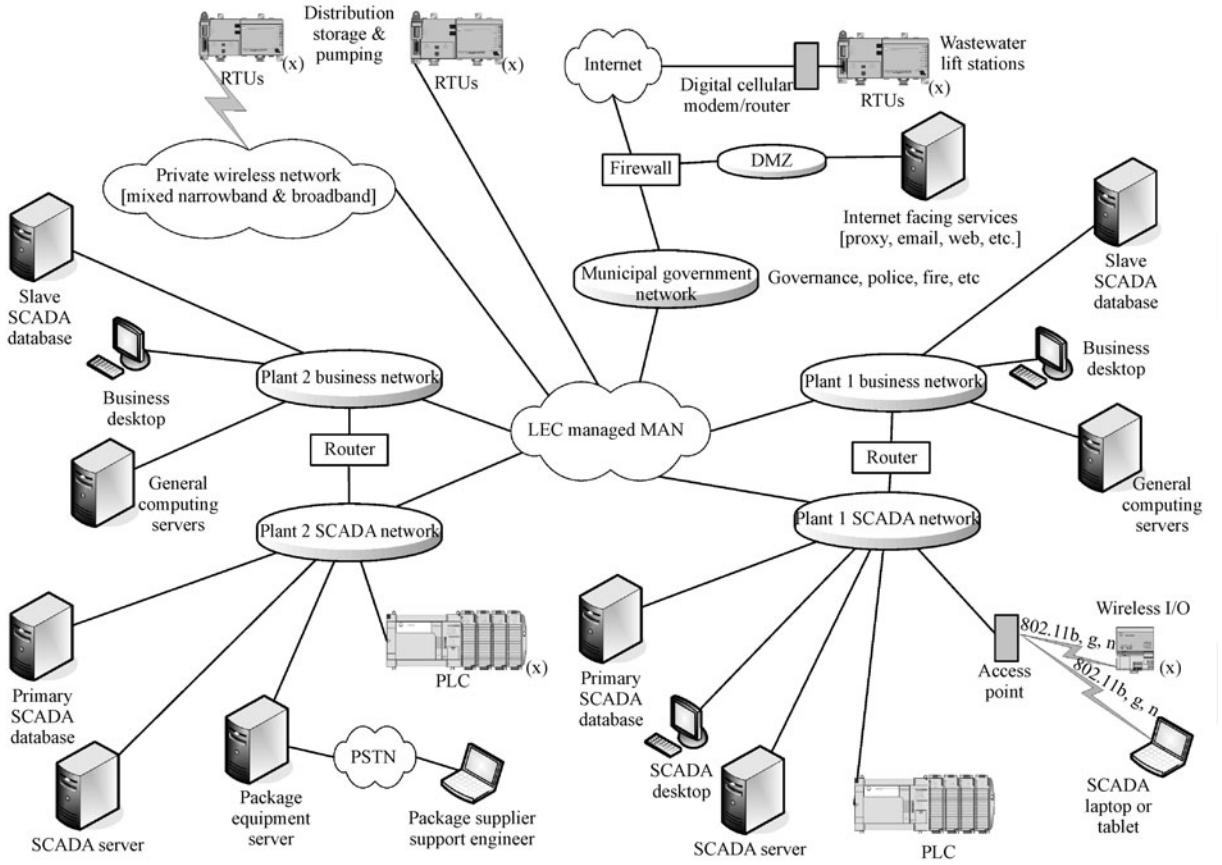

Fig. 1 Typical water/wastewater utility's business and SCADA infrastructure and network connectivity (Phillips, 2009a)

network and the utilities private wireless network. For simplicity, the LEC provided routers at MAN connections are not shown in the figure.

- A digital cellular based lift station monitoring network.
- SCADA historical databases mirror servers on the business networks to provide the business network with SCADA status data.

This utility network has a number of clearly visible vulnerabilities. Access can be gained through the business network via the Internet using a well publicized hypothetical SCADA attack (as shown in Fig. 2). The numbered callouts in Fig. 2 explain each step in the attack. To show relevance to the Water Sector from this well known vulnerability, a successful attack in this case can result in a dangerously high chemical level in the water distribution system.

As in most real-world publicized cases, a patch for this vulnerability is readily available and simply installing the patch will prevent this attack from taking place. Another longer-term security improvement that could be potentially included in a capital improvement project is to improve separation between the utility's SCADA and business networks by adding a third demilitarized zone (DMZ) subnet with a firewall connecting the three networks. Figure 3 shows this suggested improvement.

Through this improvement the direct connection requirement between the SCADA and business networks needed to provide database access for both networks has been eliminated (see dashed arched data flow lines). The firewall can also be configured to improve security for RTU digital cellular traffic routed across the Internet.

4 Cyber infrastructure—Threats, vulnerabilities and attacks

The ever increasing cyber infrastructure connectivity and the standardization of infrastructure equipment, inherently make a utility more vulnerable to cyber attacks. And while the motives of an individual or a group of attacker(s) may vary, the attack tools used and the attack methodology can be very similar. However, depending upon how well a utility's cyber infrastructure is protected, the outcomes may be very different.

The Security Incidents Organization™, a non-profit corporation maintains a Repository of Industrial Security Incidents (RISI). RISI focuses strictly on the industrial automation community. Their database includes incidents that are voluntarily reported by the user community. RISI database also includes the industrial security incident data

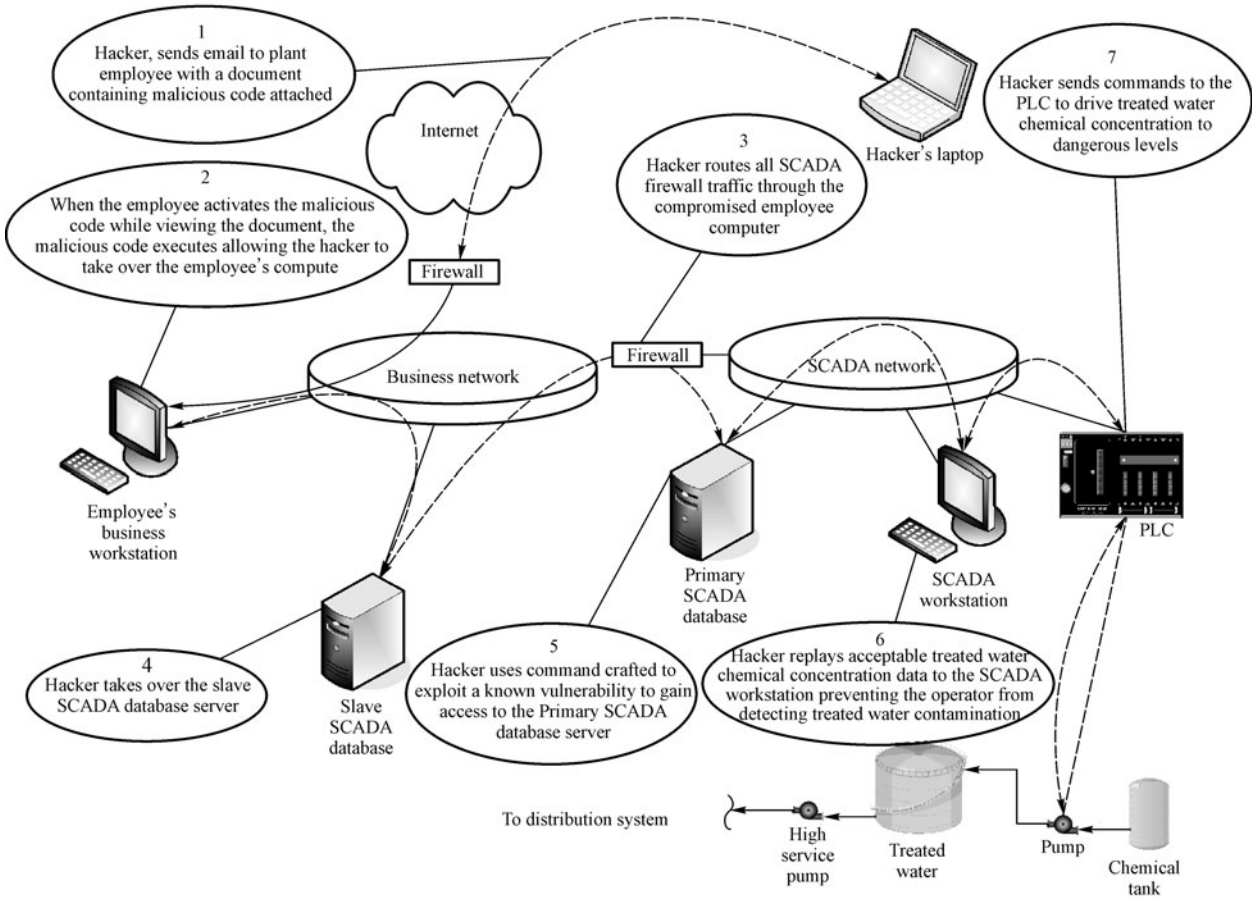

Fig. 2 SCADA network attack scenario (Phillips, 2009b)

previously collected under a research project by the British Columbia Institute of Technology (BCIT). The information presented in this section is entirely based on RISI's most recent annual report on cyber security incidents and trends affecting industrial control systems (RISI, 2010).

The number of reported security incidents related to industrial automation is increasing worldwide. The water and wastewater sector is number 4th in this list behind power, petroleum and transportation sectors (Fig. 4).

Figure 5 shows a summary global security incidents based on the documented point of entry of the attacker.

As shown in Fig. 5, a vast majority of these incidents, for which an entry point is provided, occur through either the local business network or via remote access. The economic impact of security incidents can vary widely. Figure 6 shows the financial impacts of the incidents reported in the US.

Figure 6 indicates that 23% of the industrial security incidents resulted in damages greater than one million dollars per incident. The RISI's annual report on cyber security incidents and trends affecting industrial control systems contains additional valuable information such as incident perpetrator, incident detection method, general access method, and equipment involved. Each annual report includes a detailed summary of selected security incidents. A copy of the full report can be obtained from: http://www.securityincidents.org.

5 Cyber-security standards and approaches

In recent years, many organizations have collaborated to develop standards related to cyber security. There are a number of cyber security related standards that have already been developed or that are currently under development around the world. Overall, there are three major cross-sector cyber security standards that are relevant to the water and wastewater infrastructure sector. The first and the most widely recognized world-wide standard for cyber security is the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Standard 17799 entitled, "Information Security — Security techniques — Code of practice for information security management". As the

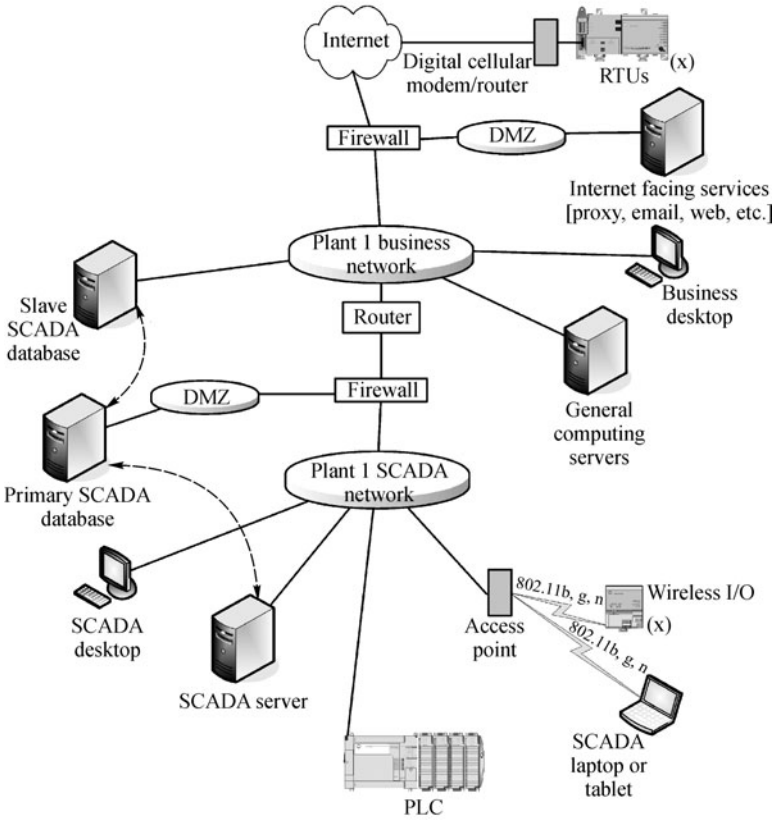

Fig. 3 Example DMZ Application to Improve Security (Phillips, 2009c)

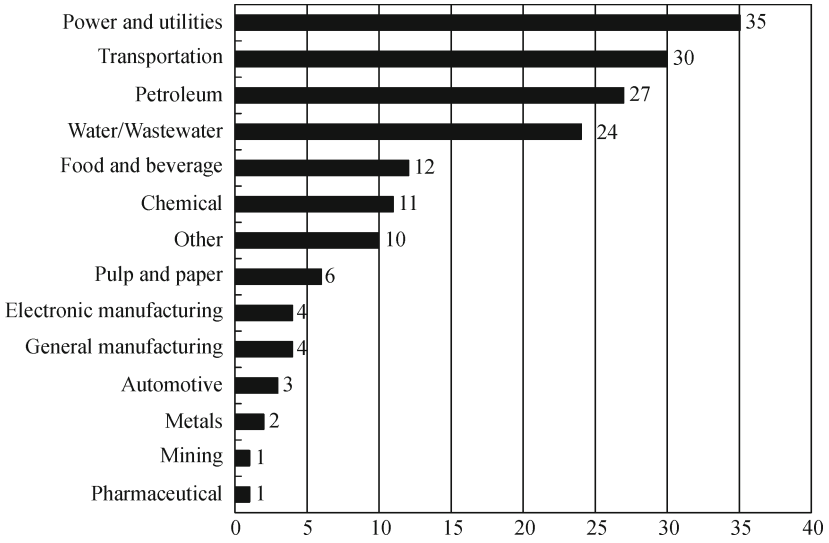

Fig. 4 Number of reported industrial security incidents in the world—Summarized by infrastructure sector (RISI, 2010)

name suggests, the standard is written for information security professionals. So, while many of the concepts can be applied to SCADA security, this standard is better suited for individuals working in information technology field than those working in industrial automation. In 2007, this standard was renumbered as ISO 27002 to better fit within the ISO 27000 Management System.

The second standard entitled, "Guide to Industrial Control Systems (ICS) Security," was published final in June 2011, by the National Institute of Science and

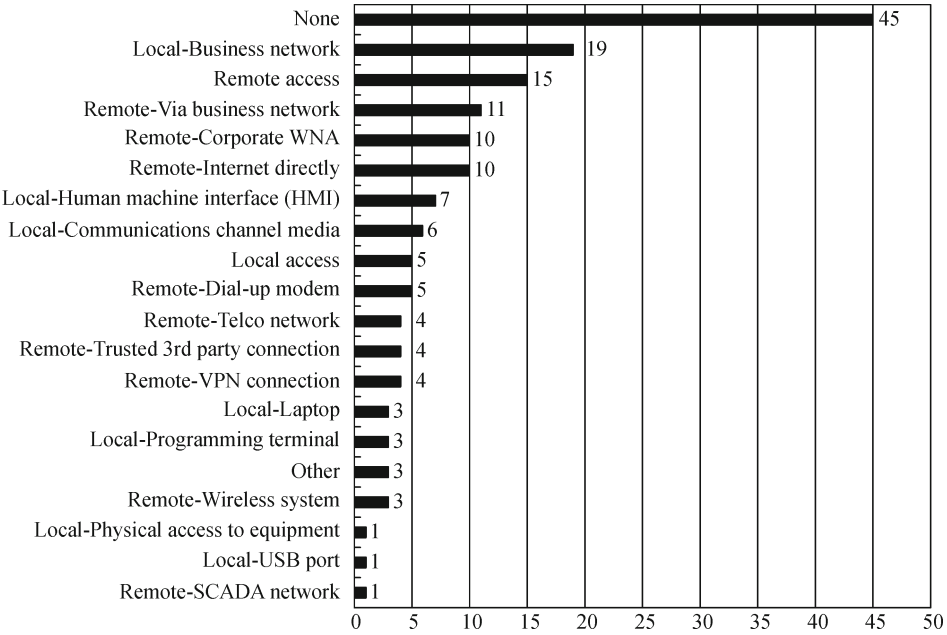

Fig. 5 Number of reported industrial security incidents in the world—Summarized by points of entry (RISI, 2010)

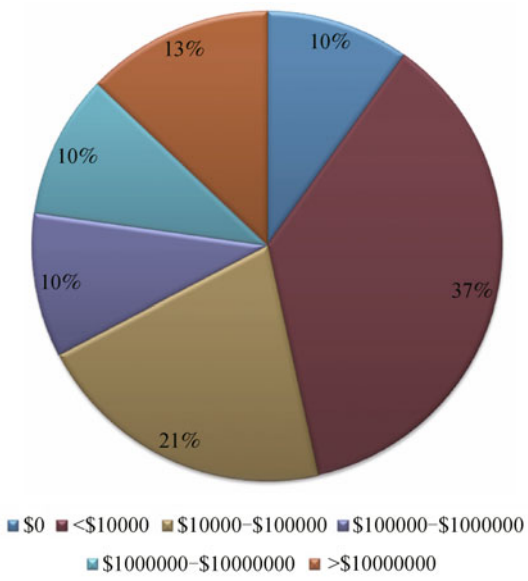

Fig. 6 Financial impact of industrial security incidents reported in the US (RISI, 2010)

Technology (NIST) as Special Publication 800-82. This standard provides particularly comprehensive control system security guidance. While this standard/guideline was specifically prepared for use by US Federal agencies, it may be used by nongovernmental organizations on a voluntary basis.

IEC's TC 65 WG 10 has joined with the International Society of Automation (ISA) 99 in producing a set of 14 international control system security standards and technical reports. One technical report and three standards have been released so far with the most recent being ANSI/ISA SP99.02.01-2009 entitled, "Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program." The third draft of ANSI/ISA-62443.03.03 (99.03.03) Security for Industrial Automation and Control Systems: System Security Requirements and Security Assurance Levels, was released for review and voting in September 2011.

Although the structure and language across the three aforementioned standards differ, the basic guidance provided is relatively consistent; and all three are applicable to the water sector. Overall, the ISO and ISA jointly developed standards released so far, as well as those yet to be released are industry independent, incorporate best practices from the aforementioned ISO and NIST standards, and are highly recommended for adoption. Depending upon the organization, for some entities, national standards such as NIST standard for US organizations may be more suitable for adoption. At a minimum, the utilities should perform vulnerability assessments (VAs) and develop emergency response plans (ERPs) to address cyber-security requirements. Based on the review they should look for opportunities to improve the following infrastructure components:

- Physical Security
- Access and Authentication Methods
- Software Improvements
- Privacy Improvements
- Network Topology Improvements

Plant operations should be designed (or redesigned) to run on local control or manual controls for extended

periods of time (3–4 days) in the event SCADA network is disrupted. All hazard scenarios including natural calamities should be evaluated to augment and improve upon the existing infrastructure. Emergency operations center (server buildings), wireless (or radio) access points should be protected. Direct connections between business and SCADA networks should be eliminated or at least minimized and protected. End point security should be implemented such that it is not possible for the cyber attacker to move data off the system.

Collective implementation of selected countermeasures is often referred to as the "defense in depth" strategy. This concept has really not changed much since the middle ages. The greatest castle-builders of their time learned the hard-way that an enemy could breach even the highest castle walls given enough time and persistence. So, they began building in layers of security that extended beyond the thick walls of the castle itself. These layers were designed to do two basic things, either expose the enemy sooner than they intended or to slow their progress, giving the kingdom more time to muster the troops.

These same concepts are employed in some of the best security plans of our day. By building in layers of protection like email filters, anti-virus, compartmentalization, authentication controls, firewalls, DMZ's, intrusion detection, and more, one can slow down an attacker's attempts. In some cases, the attacker's motivation can be reduced by making it seem as if the goal is not worth the effort it would take to capture it. The defensive layers that can be employed include:

- Secure Network Topologies
- Logical Network Separation
- Effectively Employing DMZs
- Limiting Physical Access
- Restricting Privileges

This is an important concept that when properly applied will improve the chances that any failure that does occur as a result of an attack will be more gradual and graceful allowing more time to react.

6 Funding network security improvements

One funding approach being used by US water wastewater utilities is to add cyber-security related work elements to expand and upgrade capital improvement projects. If the utility has a current VA that includes network improvements recommendations and the network is well documented, the security improvements added can be a stepwise approach to implementing the VA recommendations. Without a VA and network documentation, any security improvements implemented are still likely to improve security, but less likely to be the most effective improvements needed. General technical controls that can be funded through a capital improvement project that are very likely to improve network security include:

1) De-Militarized Zone (DMZ) — A separate small buffer network between a private internal SCADA network and an external network (Fig. 3). A DMZ can eliminate most direct connections between the internal and external networks while providing external access to the information from the SCADA network.

2) Intrusion Detection Systems/Intrusion Protection Systems (IDS/IPS) — Network-based Intrusion Detection Systems (NIDS) examine network traffic in more detail than routers and packet inspection firewalls, and block suspected malicious traffic. They use a range of detection algorithms to detect and log suspicious network traffic. IDS/IPS technology is constantly improving and a single NIPS can protect the whole SCADA system. However, intrusion detection and protection systems still can generate a lot of false positives that increase maintenance support requirements and can restrict network traffic when they become overloaded.

Host-based Intrusion Protection Systems (HIPS) that must be included with the operating system or included as part of a third-party virus protection package are also available. However, like the virus protection application, host-based intrusion protection consumes resources on each workstation and server and can impact ICS responsiveness. Also, host based systems require updating and maintenance on each host which can be maintenance intensive.

3) Role-Based Access and Single Sign-on — Role-based access control uses computer operating system and application group user policies to limit access to information to that required to support the role of the user. Single Sign-on eases user account and group policy management.

4) Wireless Network Access Controls — Using standards-based virtual private network (VPN) technology to provide encryption and authentication mechanisms to discourage intrusion and limit access to wireless networks combined with other network protection techniques to reduce the vulnerability of wireless networks. Wireless network access controls and encryption are critical for broadband wireless networks with direct network connections.

7 Conclusions

Cyber attacks are real and can cause significant damages. Water and wastewater utilities must adopt countermeasures to prevent or minimize the damage in case of such attacks.

The utilities must perform vulnerability assessments and develop necessary emergency response plans. The utilities must voluntarily select and adopt security standards and countermeasures that best meet their security and organizational requirements. The utilities should optimally utilize their limited funding resources to prepare and implement necessary programs that are designed to

increase cyber-security over the years. Utilities should also get creative and allocate more funding through annual budgets rather than depend solely upon capital improvement programs to achieve improvements in cyber-security.

References

Abrams M, Weiss J (2008). Malicious control system cyber security attack case study—Maroochy water services. The MITRE Corporation, July 23, 2008. Available at: http://www.mitre.org/work/tech_papers/tech_papers_08/08_1145/08_1145.pdf

ISO/IEC 27002 (2005). Information Technology — Security Techniques —Code of Practice for Information Security Management (Redesignated from ISO/IEC 17799:2005 in 2007). Weissman O (Germany) Plate A (UK), eds. International Organization for Standardization, Geneva, Switzerland, 2007

Panguluri S, Phillips W R Jr, Ellis P (2011). Handbook of Water and Wastewater Systems Protection, Chapter 16—Cyber Security: Protecting Water and Wastewater Infrastructure. Clark R M, et al. eds. Springer Science_Business Media, LLC 2011

PBS (2004). Frontline program titled "Cyber War!" Airdate: April 24, 2003, http://www.pbs.org /wgbh /pages /frontline /shows /cyberwar/

Phillips W R Jr (2009a). Typical water/wastewater utility's business and SCADA infrastructure and network connectivity. Copyright 2009 by CH2M Hill. Reprinted with Permission

Phillips W R Jr (2009b). SCADA network attack scenario. Copyright 2009 by CH2M Hill. Reprinted with Permission

Phillips W R Jr (2009c). Example DMZ application to improve security. Copyright 2009 by CH2M Hill. Reprinted with Permission

President's Commission on Critical Infrastructure Protection (PCCIP) (1997). Critical Foundations: Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection, October 1997

Repository for Industrial Security Incidents (RISI) (2010). Annual Report on Cyber Security Incidents Affecting Industrial Control Systems—Annual Report 2010. Available from RISI at: http://www.securityincidents.org