

Critical Infrastructure

Part II: Drinking Water and Waste Water Treatment Systems

Authors:

Will Gragido, CISSP CISA | NSA-IAM/IEM |

John Pirc, CEH | NSA-IAM | SANS Security Thought Leader

Jonathan Amato, CISSP

Scott Lupfer, CISSP, GIAC –CIH

Ian Gorrie, CISSP, CISM, CISA, ISSAP, C|EH

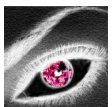
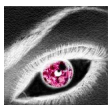


Table of Contents

Introduction	3
Water	4
Types of Water Systems.....	6
Drinking Water System Assets & Components	7
Physical Elements	7
Cyber Elements.....	7
Human Elements	8
Department of Homeland Security (DHS) Sector-Specific Plan (2006)	8
National Infrastructure Protection Plan (NIPP).....	9
Examples of Vulnerability and Exploitation of the Water Sector.....	11
Relevance of SCADA in Water Sector (Drinking Water and Waste Water).....	14
A Word about Supervisory Control and Data Acquisition (SCADA) Systems	14
What Makes SCADA Systems So Vulnerable to Attack and Exploitation?	15
Impact of Vulnerability of Water Sector on Critical Services.....	16
Conclusion.....	18
Sources:	19



Introduction

In the first installment of this series, we established that our world and times are complex – far more complex than perhaps than our ancestors or ourselves ever envisioned. Marked by evolutionary thought and action in commerce, foreign affairs, communication and interactivity, a quantum leap has been realized; a pivot point set in place which will see humanity evolve throughout the remainder of the 21st century and beyond. We the authors believe that because of these changes, this evolution revolution, the world has become a place that sees and recognizes the need for checks and balances more so than ever before. Non-negotiable in nature, they are more important now than perhaps ever before. The balance described above is applicable to all human life (and by virtue of this, all life on the planet that engages humanity in even the smallest ways). Ensuring this balance, in addition to sustaining it, involves safeguarding the infrastructure upon which it depends. Here in the United States of America we have official and unofficial voices crying out for measures just such as this to be implemented. The ***Homeland Security Presidential Directive (HSPD-7)*** designates the Environmental Protection Agency (EPA) as the Sector Specific Agency (SSA) for the Water Sector. HSPD-7 defines the following Critical Infrastructure/Key Resource (CI/KR):

- **Information technology**
- **Telecommunications**
- **Chemicals**
- **Transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems**
- **Emergency services**
- **Postal and shipping services**
- **Agriculture, food (meat, poultry, egg products)**
- **Public health, health care, and food (other than meat, poultry, egg products)**
- **Drinking water and waste water treatment systems**
- **Energy, including the production refining, storage, and distribution of oil and gas, and electric power**
- **Banking and finance**
- **National monuments and icons**
- **Defense industrial base**

The balance of life in all geographies—developed nations, developing nations, urban areas or rural is dependent upon some form of these Critical Infrastructure / Key Resources (CI/KR) first existing, second being safeguarded, third being made available and fourth being preserved. Though some might argue that not all within this list are ‘critical’ to a people’s or nations existence – national monuments and icons for example (though these are considered critical in the opinion of the authors due to the frequency of tourism, traffic, transportation etc.), their significance to modern society cannot be ignored nor should their relevance. Should one or more of these identified elements of Critical Infrastructure / Key Resources (CI/KR) be irrevocably damaged, the impact upon humanity (and our way of life and the world as we know it), would be difficult to assess much less describe; even in light of previously conducted impact analysis exercises, which yield both quantitative and qualitative data. In Part I of this series we questioned whether or not an occurrence or event of interest, conducted in simulation or in reality would see humanity (regardless of its geo-location), take stock in its investments (and itself), ultimately culminating in the refocusing and redirection of its resources and energies. This is neither a simple question nor a simple premise. It forces us to ask ourselves whether we possess the where with all necessary to demonstrate grace under pressure in the event we are called upon to do so. We



concluded that human life relies upon its infrastructure – physical, emotional, spiritual, philosophical due to the vital nature it plays in our survival and the proliferation to our species as residents on planet Earth. We believe it has been this way since the beginning of time.

Our position suggests that this reliance is woven into the tapestry of our ancestry, our lives and futures. It is the logical advancement of maturity and adaptation, which is to have been expected of humanity as he transitioned from nomadic hunter-gathers to agrarian domesticated farmers. It reflects the natural conscious or subconscious desire of all human beings to see our species successfully grow and preserve itself as opposed to seeing it be obliterated in some Darwinian sequence. Our assertion is that it is futile to argue against these most basic and elementary assertions and to do so is illogical, much less absurd.

Water

The importance of water cannot be stressed enough in the context of discussions such as this one. Clean, fresh drinking water is vital to humanity's existence as well as to other forms of life on planet Earth. It is essential. Without it, nothing that lives outside of the seas, can survive. Albert Szent-Gyorgyi, the famed biochemist once said of water, "Water is life's mater and matrix, mother and medium. There is no life without water." Water appears in all three physical states of matter (solid, liquid, gas). Additionally, it appears in a variety of forms here on Earth, including:

- Water vapor
- Clouds in the sky
- Sea water
- Glaciers
- Icebergs
- Rivers, streams, creeks
- Aquifers
- Reservoirs and lakes

Understanding its global prevalence and geo-location is important because of the role (as we have mentioned earlier) that water plays within our world. In developed nations, we understand the impact water has on our lives. From healthcare to agriculture to manufacturing, water has a significant impact on our development as humans and industrialized nations. However, consider the following facts from UNICEF (2008):

- 1.5Million children per year die from diarrheal diseases, which are attributed to lack of adequate sanitation
- 2.5Billion people lack access to improved sanitation
- 1.2Billion people have no access to any form of sanitation facilities
- 884Million people do not have access to safe drinking water
- In Sub-Saharan Africa in 2006 only 31% of the population had to improved sanitation and only 58% had access to some form of improved water system

This paper is not intended to address how to solve these statistics or others like them; rather these facts are included by the authors to ensure our audience considers the need to protect the infrastructure of our potable water and sanitation systems. The authors decided to select data specifically from Sub-Saharan Africa due to the fact that there are many countries in that part of the world that have



experienced their share of atrocities, civil wars, unrest and other forms of violence in the past decade. Some of these familiar names are:

- Sierra Leone
- Ivory Coast
- Congo
- Somalia
- Darfur
- Chad

While it is beyond the scope of this document or the research performed by the authors for this work, it may be concluded that a lack of quality drinking water and sanitation facilities may have contributed to the strife and / or conflicts in theater. The lack of such resource may have (and in some cases has), contributed to the escalation of these conflicts contributing to more deaths due to starvation and thirst than may have been experienced otherwise. According to the World Health Organization (WHO) a study conducted in 2005 demonstrated that, in poor countries with improved access to clean water and sanitation, an average 3.7% annual economic growth was realized. Clearly, access to potable water has a direct economic impact. Using the Sub-Sahara Africa example, we must ask ourselves; if these countries had greater access to potable water and quality sanitation systems, would there be less civil unrest and more participation in a local or global economy by their population? Again, the answer to this question is not the scope of this document, but it may help us understand how our own economies, civil peace and civilization could be negatively affected should we suddenly not have access to clean water.

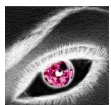
Using the above statistics and examples of strife and warfare in regions without adequate sanitation and water facilities, ask yourself the following questions:

- What if the availability of *clean, potable* water for consumption or use by human beings, animals, or plant life in an industrialized nation was threatened or suddenly ceased to exist?
- What might the repercussions be should something occur which temporarily or permanently affected a given source of fresh water?

Access to safe drinking water has improved the world over and as a result, the correlation between clean drinking water and a nation's Gross Domestic Product (GDP) can be seen per capita. However what if something occurred to threaten that?

- How would your business change if suddenly you were added to the population of those without access to potable water and adequate sanitation systems?
- Can water become a commodity valuable enough over which wars are fought?
- What would the impact be on the world economy were there a significant reduction in potable drinking water or the facilities which enable us to create potable water?
- How would your community, city, region, country or continent change if significant numbers of the population suddenly lost access to clean water and sanitation due to a failure in the physical and cyber security of those facilities that ensure access to those resources on a daily basis?

Our assertion is that the impact would be severe and costs great. Consider the following statistics provided by the **Department of Homeland Security (DHS)** and **Environmental Protection Agency (EPA)**, in a paper titled **Water Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan May 2007:**



- There are approximately 160,000 public drinking water utilities and more than 16,000 wastewater utilities in the United States.
- About 84 percent of the U.S. population receives its potable water from these drinking water utilities and
- More than 75 percent of the U.S. population have their sanitary sewage treated by these wastewater utilities
- The drinking water and wastewater sector (Water Sector) is vulnerable to a variety of attacks, including contamination with deadly agents and physical and cyber attacks.
- If these attacks were to occur, the result could be large numbers of illnesses or casualties or denial of service that would also affect public health and economic vitality
- Critical services such as firefighting and health care (hospitals), and other dependent and interdependent sectors such as energy, transportation, and food and agriculture, would suffer negative impacts from a denial of Water Sector service
- In collaboration with the entire sector, a broad-based strategy to address security needs is being implemented
- This work includes providing support to utilities by preparing vulnerability assessment and emergency response tools
- Providing technical and financial assistance, and exchanging information

Types of Water Systems

According to a publication titled *Safe Drinking Water Information System, Federal Version*, published in January 2004, there are three primary types of systems associated with drinking water. Those systems are:

- Community Water Systems (CWS)
- Non-transient, non-community water systems (NTNCWS)
- Transient non-community water systems (TNCWS)

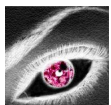
Community Water Systems (CWS) are public water systems that serve at least 25 year-round residents or 15 connections to year-round residents. Non-transient, non-community water systems (NTNCWS) are public water systems that regularly supply water to at least 25 of the same people at least 6 months per year, but not year-round. Examples of NTNCWS' include:

- Schools
- Factories
- Office buildings

Transient non-community water systems (TNCWS) are public water systems that service environments such as:

- Campgrounds
- Gas Stations

TNCWS' traditionally focus on servicing a transient population at least 60 days per calendar year.



Drinking Water System Assets & Components

Drinking water assets contain many components and elements. They are described as physical, cyber and human elements. In the following sections, we will delve more deeply into what contributes to these components and elements and what threat vectors may be associated with each.

Physical Elements

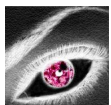
The physical elements of these assets and components are generally comprised of the following:

- **Water source:** May be groundwater, surface water or a combination of the two. According to the NIPP, the vast majority of the CWSs serving fewer than 10,000 people use groundwater as their primary source. In cases where CWSs are serving more than 10,000 people routinely, the source for primary use will most often be a surface water source.
- **Conveyance:** The process of delivering water from a source to a treatment facility. CWS's use large pipes or open canal systems to do this. The water is either pumped or gravity-fed through these systems.
- **Raw Water Storage:** Most often reservoirs or tanks are used to hold water from the source prior to treating it. Reservoirs or tanks can be remote or located within urban areas.
- **Treatment:** Using a variety of physical and chemical mechanisms to treat the water, contaminants are detected and removed from the raw water in order to safe guard and guarantee it is potable.
- **Finished Water Storage:** Post treatment, water is stored prior to being distributed to its customers. Though limited, there are cases where treated water is stored in large, uncovered tanks or reservoirs making them potentially susceptible to attack and contamination.
- **Distribution Systems:** Immense, convoluted networks of pipes, tanks, pumps, and valve systems that aid in conveying water to customers. Flow is adjusted to ensure that the proper volume and pressure is delivered when and where needed throughout the network.
- **Monitoring Systems:** Monitoring is traditionally conducted with emphasis being given to conventional regulated and unregulated contaminants. Some facilities utilize advanced sensors, place strategically throughout their infrastructure, to monitor a wide range of physical properties including but not limited to water quality and pressure

Cyber Elements

The cyber assets and components of these systems are generally comprised of the following:

- **Supervisory Control and Data Acquisition (SCADA) system:** Some utilities have Internet Protocol (IP) enabled, electronic networks, often including wireless communication, to link the monitoring system, and controls for the treatment and distribution systems, to a central display and operations room. It should be noted that these systems are designed to do the following:
 - Help automate control of a drinking water utility with monitoring system readouts serving as inputs for control.
 - SCADA systems are part of integrated control systems essential to operation of drinking water utilities.



Human Elements

The human assets and components of these systems generally include the following:

- **Employees, Consultants and Contractors:** Drinking water utilities, like many businesses, utilize and depend upon a wide variety of employees. These include part-time, full-time, and contract employees who bring skills necessary to manage and operate these facilities in normal and abnormal operational scenarios.
- **Types of Roles:** All environments require that either one or more resources address a variety of roles and job functions. In larger environments and facilities these job roles and requirements must be filled by highly trained and fully qualified professionals. Examples include but are not limited to the following:
 - Chemists
 - Engineers
 - Microbiologists
 - Public Relations
 - Security Personnel
 - Other specialists
- **Role of Consultants & Contractors:** Consultants, contractors and other third parties within these environments can play key roles with respect to:
 - Engineering services
 - Laboratory analysts
 - Chemical delivery systems
 - Security services

All of which are required to ensure the integrity and availability of the facility and its product. This is extremely important when considering that drinking water facilities differ in the type of components used, age and upkeep of these components and infrastructure, and that some utilities might not have all the components discussed previously.

Department of Homeland Security (DHS) Sector-Specific Plan (2006)

The Department of Homeland Security (DHS) in their 2006 Sector-Specific Plan outlined eight sections, which describe and clearly articulate its guidance for providing safe, secure drinking water and water treatment facilities. The following list describes each section of the **Sector-Specific Plan** that will be described in detail later:

1. **Sector Profile and Goals** -- This section of the Sector-Specific Plan (SSP) provides an overview of the Water Sector
2. **Identify Assets, Systems, Networks, and Functions** – This section of the Sector-Specific Plan (SSP) discusses ongoing efforts by government agencies and Water Sector security partners in accomplishing the following with respect to critical assets which if compromised, impact the economy or public health:
 - a. Identify

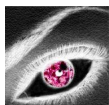


- b. Prioritize
 - c. Coordinate
- 3. **Assess Risks (Consequences, Vulnerabilities, and Threats)** -- Describes the Water Sector's approach for assessing risk, which is the measurement of potential harm due to threat, vulnerability, and consequence. Assessment of risk is of paramount importance to assessing readiness or identifying deficiencies.
- 4. **Prioritize Infrastructure** -- The Department of Homeland Security (DHS) requests that the Water Sector describe the process for risk-based prioritization of its assets. This of course, requires the identification of assets, systems, networks, and functions in addition to the identification of threats and vulnerabilities (their associated consequences), and risk indicators.
- 5. **Develop and Implement Protective Programs**—The section discusses how the Water Sector develops and implements protective programs that are used throughout the sector, and focuses on efforts to identify, assess, select, and implement protective programs and on EPA's role in facilitating implementation of such programs
- 6. **Measure Progress**—Within this section, part of the NIPP risk management framework is discussed. The Department of Homeland Security (DHS) focuses on using core metrics to measure progress across all CI/KR sectors. The Environmental Protection Agency (EPA) is responsible for measuring progress in the Water Sector using additional sector-specific metrics.
- 7. **CI/KR Protection Research and Development** -- This section of the Sector-Specific Plan (SSP) focuses mainly on the Research and Development (R&D) initiatives conducted by EPA's National Homeland Security Research Center, and on the center's coordination and collaboration with sector R&D partners. Also depicted in this section are the management process for implementing and maintaining research activities and how the sector's vision, goals, and R&D efforts align with the nine critical infrastructure protection (CIP) R&D themes and three CIP R&D goals outlined in the National CIP (NCIP) R&D Plan
- 8. **Managing and Coordinating SSA Responsibilities**—This section of the Sector-Specific Plan (SSP) details many of the management and coordination activities that will be performed in order for the Water Sector to better protect critical infrastructure

National Infrastructure Protection Plan (NIPP)

Under Homeland Security Presidential Directive 7 (HSPD-7), certain Federal agencies must identify and prioritize critical national infrastructure and resources for protection from terrorist acts, which could cause the following:

- Catastrophic health impacts
 - Outbreaks
 - Introduction of pathogens – airborne, waterborne, agrarian or blood borne
- Mass casualties
 - Physical casualties resulting in serious injuries and loss of life
- The undermining of public confidence
 - Capitalizing
- The disruption of essential government functions
 - Communication
 - Military
 - Federal Law Enforcement

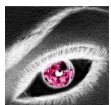


- Department of Justice
- Department of Homeland Security
- The disruption of essential services such as the following:
 - Police
 - Fire
 - Ambulatory
 - Medical
 - Communications
- Disruptions to economic activity and markets:
 - Commodities markets
 - Futures markets
 - Stock and bonds markets
 - Banking systems
 - Credit systems

As a result, a key requirement of HSPD-7 was to develop a strategy to protect all Critical Infrastructure / Key Resources (CI/KR). That strategy is known as the **National Infrastructure Protection Plan (NIPP)**. The goal of this plan is to promote a safer, more secure nation. NIPP itself follows the Department of Homeland Security (DHS) risk management framework, which describes in detail the processes for the following:

1. Setting security goals for CI/KR
2. Identifying CI/KR assets
3. Assessing the risk to the CI/KR
 - a. Consequence analysis which is the SSA's responsibility with additional guidance being provided by the Department of Homeland Security (DHS)
 - b. Vulnerability assessments which are the joint responsibility of both the SSA's and Water Sector
 - c. Threat analysis which is provided by the Department of Homeland Security (DHS), Intelligence community, and law enforcement agencies
4. Describes processes for prioritizing CI / KR
5. Implementation of programs to protect CI / KR
6. Metrics for measuring effectiveness of CI/ KR

Each Sector-Specific Agency (SSA) is required to develop a Sector-Specific Plan (SSP) that follows and supports the framework in detail. SSPs are the implementation plans that articulate strategy in a specific sector. The guidelines defined and articulated within the HSPD-7 have been written in such a way to ensure that the emphasis is placed on the terrorist threat to the United States infrastructure and resources. This meets the guidelines set for via the NIPP. The NIPP addresses a variety of areas. Special attention exists within the NIPP to the area of risk management and the subsequent creation and implementation of a framework of a national level. At the time of this writing, it is unclear whether the NIST standards shall be the standard from which this frame is developed. Within this framework, special consideration has been placed upon the physical, cyber, and human elements of the infrastructure during implementation.



Examples of Vulnerability and Exploitation of the Water Sector

We know that biological warfare has been practiced the world over, repeatedly throughout history with great success. The exploitation of food and water supplies by means of deliberate poisoning via infectious materials (excrement, blood borne pathogens), microorganisms, toxins, humans and / or animals – living or dead were commonly head practices. Claims have been made which suggest that the ancient Assyrians—who we know today were aware of infectious fungi such as *ergot*, used it to poison the wells of their enemies. Similarly, we know that the Athenians in 590 B.C. used *hellbore* – a poisonous plant, to poison wells during the First Sacred War in Greece. In many respects, we can conclude that via historical record this practice and others similar to it were universal throughout the history of man and remain so to this day.

These tactics have been used more recently, as well. Beginning in 1937 and continuing throughout the Second World War, the Japanese Army maintained a unit in Manchuria, the “Epidemic Prevention and Water Purification Department”, also known as Unit 731. Despite the euphemistic name, Unit 731 was in fact a chemical and biological weapons research facility. Among the many experiments conducted, there was an experiment to transmit intestinal typhus via public water supplies. The weapons deployed there are known to have been used in a non-experimental fashion on a public water supply on one occasion, during the Battle of Khalkhin Gol (also known as the Nomonhan Incident) Gold (2003). In 1939, a battle between the Japanese and the Soviet Union over a border region between Mongolia and Manchuria broke out. One of these battles became infamous amongst military historians, the Battle of Khalkhin Gol due to the introduction of bio-weapons in the water supply.

Throughout history, attacks against water systems have been used as scorched-earth retreat tactics as well. In May of 1945, during the German Army’s final retreat from Czechoslovakia, a large reservoir in Bohemia was poisoned with sewage, rendering the water unusable for as long as one year afterward. In more recent history, examples of the exploitation of both water and food supplies by aggressors utilizing traditional techniques akin to those described above and modern day technological ones have been noted as well Christopher, et al (1997). In some respects, the threat of such activity is equally if not more frightening, than the actual exploitation. In July of 2002, the Federal Bureau of Investigation (FBI) issued a series of warnings regarding the possibility of terrorist attacks against American targets, specifically the nation’s water utilities and facilities. The FBI had reason to believe that pumping stations and pipes that served both cities and suburbs were at risk due to the discovery of documentation in Afghanistan, which indicated that al Qaeda operatives had been actively investigating ways to disrupt or destroy the nation’s water supply on a colossal scale.

At the time, these warnings were based on sound intelligence gathered abroad in addition to previously obtained information that the FBI had gathered and released in January of 2002. This information corroborated that which was gathered previously and suggested that al Qaeda operatives had been actively investigating means by which to remotely – via the internet primarily, gain control of the United States’ water supplies and waste treatment facilities. A thought that, at the time, seemed improbable yet plausible. Years prior to this revelation being made, United States government officials stressed the ease with which the American infrastructure could be attacked and exploited to bitter ends. For this reason during the Presidency of William Jefferson Clinton, Presidential Decision Directive 63 was borne. Presidential Decision Directive 63 was conceived with the goal of ensuring the protection of the United States’ infrastructure with prejudice.



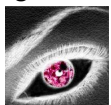
The events of September 11, 2001 saw an uptick in activity of just such protective action. The United States Coastguard implemented increased frequency in patrolling areas deemed strategic to the fresh water supplies. Cities such as Chicago experienced such increased activities. In New York City, officials dramatically increased the number of daily water supply samples collected and analyzed taken at their 900 locations from roughly 2,060 to 2,500. Other tactics were taken as well to protect these water resources including the restriction of access to roads that the authorities deemed critical to the safety of reservoirs and water treatment facilities. In 2002, the Information Analysis and Infrastructure Protection Division of the Department of Homeland Security revised their activities to meet these needs as well. The IAIPD took the following measures to curtail potential risks: All facilities (treatment plants, reservoirs, reservoir dams, water storage facilities and towers, pumping stations, water intake facilities, chlorine booster stations, and meter and valve boxes) should be fenced, be well lighted, and have a perimeter that is monitored by surveillance cameras and motion detectors.

To prevent hacking, supervisory control and data acquisition systems for monitoring and controlling water parameters should not be connected to the Internet. Remaining cyber security should be enhanced, and passwords should be changed regularly. The EPA should give grants to cities to ensure fire hydrants and other entry points to the distribution system are tamperproof. Surveillance cameras should be located on-site at key points, such as at the chlorine storage facilities, chlorine injection areas, filter beds, hazardous chemical and fuel storage areas, and finished water storage areas. In 2002, much debate took place as to whether or not water authorities nationally, had taken the initiative to conduct full-scale vulnerability assessments.

Some water treatment professionals dismissed the need for such activity citing that the real threats to our water supplies were the aging and eroding pipes and components that deliver water to our population. However, despite the controls put in place the lingering question as to whether or not they would be sufficient in order to prevent vandalism or terrorism equating in compromise of our drinking water and sewage treatment facilities remained unanswered. The United States however is not alone in this predicament. Nations the world over face similar challenges and, as time progressed saw the realities of terroristic acts and threats increase with respect to these systems.

In 2008, federal investigators reported that a jihadist website had posted a call to poison the water supplies of major cities the world over. Additionally, that same site called for jihadist attacks on what the messengers called "atheist Europe" which many believe to be a thinly veiled reference to the entire West. Days after the postings were discovered a Canadian immigrant, 29 year-old Saleman Abidirahman Dirie, was found dead in a Denver, Colorado hotel room with a pound of cyanide intended, according to investigators, for the Democratic National Convention. A great deal of speculation rose from these cases regarding whether or not they were related or coincidental. Investigators and members of the intelligence community took opposing views on the matter with respect to the seriousness and probability associated with it. . However, the FBI's primary informant this case, Dirie was found dead due to the ingestion of poison with no real explanation as to what led to his end or why. Official comments regarding the threat to the water supply of the United States, specifically that which would have affected the Democratic National Convention, were deemed "aspirational" as opposed to "operational" however, the intent to encourage and carry out such action was clear to law enforcement and intelligence community members.

The year 2008 saw additional threats from jihadi internet forums and sites regarding terrorist plots against the United Kingdom and Denmark. These plans called for the use of both chemical and



biological agents to contaminate water resources throughout the region with Denmark targeted specifically due to the perceived insults against the Prophet Muhammad made via the publication of the infamous “Muhammad Cartoons”. The posts shared a common title “Back Breaking Blow to Denmark, the U.K. and the European Union” all discussing ways in which to carry out these strategies and plots in retribution. Baghdad al-Khilafa, a forum member with over a thousand postings -- primarily on weapons and explosives, proposed the terror attack to retaliate for the following:

- Denmark’s mockery of the Prophet Muhammad
- To terrorize the enemy’s ranks
- Ease the infidels’ onslaught on Muslims in
 - Iraq
 - Afghanistan
 - Morocco
 - Somalia
 - Eastern Turkistan (Xinjiang)
 - Chechnya

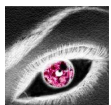
The plans objectives were clear:

- Kill as many civilians as possible by contaminating the main water supply pipelines in any of the major cities in Europe with biochemical substances.
- The stages outlined by Baghdad al-Khilafa reflected the following intentions:
 - Collect intelligence on the target and determine the right timing for execution. This involves reconnaissance, casing facilities and frequenting the target country.
 - Distract and avoid security forces at the target. A mock operation is created to divert attention from the original target.
 - Use one fair-skinned blond jihadi to execute the attack and leave the country immediately after perpetration.
 - Use a highly poisonous chemical substance to contaminate the water supply.

The terror plot stirred strong interest among forum participants who requested execution plans, ways to reach the target country and further details on producing the chemical substances. In addition to aiding in the formulation of this plot against the water supplies of Denmark, the United Kingdom and the European Union, a list of the materials and substances to be used in the attack was made public to the forum participants. The list included:

- Cyanide
- Hydrocyanic acid
- Potassium cyanide
- Aniline hydrochloride
- Sodium nitrite
- Cobalt
- Thallium --a highly toxic chemical compound colloquially referred to as the “poisoner’s poison”

In addition to these compounds, poisonous gases such as chlorine gas, mustard gas, hydrogen cyanide and nerve gas were also suggested and added to the listed of desired materials. Distribution methods were discussed, along with photos of pumping stations, water pipelines, water towers and diagrams detailing and illustrating ways to introduce these compounds into the water supply. One suggestion,



made by a mechanical engineer and active jihadist forum participant involved using the valves and ventilation openings as points of entry. In November 2009, the Pakistani Taliban threatened to contaminate the water sources and reservoirs with toxic materials in order to place pressure upon the army to stop military operations against them in South Waziristan tribal region. The water authorities and cantonment boards of Rawalpindi and Chaklala received the threats from the banned Tehrik-e-Taliban Pakistan in the form of a faxed letter. The group claimed to have access to in excess of 200 liters of poisonous materials that they would use to contaminate the water supplies if their demands were not met. Pakistani authorities confirmed the reports and stated that they had taken “effective security measures” to prevent any such activity.

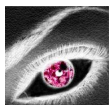
SCADA Security in Water Sector (Drinking Water and Waste Water)

A Word about Supervisory Control and Data Acquisition (SCADA) Systems

No conversation having to do with critical infrastructure (CI) and / or key resources (KR) would be complete without addressing the Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems were originally designed to provide real-time control and monitoring of utility specific distribution systems. Drinking water and water treatment systems are no exception. As such, it is considered by the authors non-negotiable that these systems are protected both physically and logically without exception. Though best practices and standards exist for the express purpose of governing the design, implementation and operation of these systems it is often the experience of auditors and assessors, including some of the authors that these systems are found to be in ‘violation’ of the most rudimentary elements of SCADA related (FERC CIP) governance. The authors are not alone in this experience as several other competent auditors, assessors and security researchers have found this to be the case as well. In 2006 at Black Hat Federal, then IBM Internet Security Systems employees and X-Force Research Team members Robert Graham and David Maynor gave a compelling presentation on SCADA systems (as they the authors of the presentation, in addition to other members of the IBM ISS Professional Services and Research teams), had experienced them. Within the context of their presentation, Graham and Maynor deftly articulated many of the rumors and claims, which had achieved notoriety up to that point the world over in addition to interjecting their own views and conclusions representing the culmination of their collective previous five years worth of experience. Their conclusion was this:

- There was neither cause to panic nor to ignore the issue
- Their experience penetrating systems led them to believe it should be taken seriously

The authors of this paper concur with Graham and Maynors' findings. Furthermore, we suggest that since the time of Graham and Maynor’s presentation in 2006, the situation has been more grave and instances where awareness was lacking which resulted in compromise and exploitation have increased. As a result, the authors felt it appropriate to describe SCADA systems vulnerability to attack and exploitation without devoting the entirety of this document to that subject. In the following section, we will explore some common elements of weakness associated with SCADA vulnerabilities and exploitations.



What Makes SCADA Systems So Vulnerable to Attack and Exploitation?

It is important to take a moment to discuss what, exactly, makes SCADA systems so vulnerable to attack. With respect to SCADA systems, they suffer the same potential issues any system would were they not properly assessed for risk from a physical and logical perspective. In an ideal world, this assessment would occur prior to deployment of any system on a network however this is most certainly not the case in SCADA or non-SCADA systems. As a result, the associated attack surface of these systems and their environments grow to meet their level of susceptibility to both threat and vulnerability.

Though there may be more potential areas of deficiency associated with SCADA systems and environments from a security perspective, the following nine areas of deficiency are useful for generic categorization and grouping. It should be noted that the author's intention by including these categories is to provide insight into the areas that suffer more frequently within these environments and as a result are more likely to be exploited or faulted rather than asserting that these represent the entirety of all threat vectors associated with SCADA systems and environments.

Application Coding Deficiencies

In many environments where SCADA systems are deployed it has been noted that a fundamental contributor to the deficiencies found in overall risk posture stem from poor application development and coding practices. SCADA systems are not unique in this sense however, given their intended use and mission criticality, it is extremely important to note just how serious these issues are. Examples range from the presence of buffer management issues to substandard string handling. In many cases, this translates to these systems are being deployed in a vulnerable state.

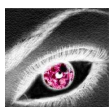
Additionally, issues pertaining to the use and exploitability of batch files, scripts, and interface programming languages found present within these environments creates an even more unstable posture. The result of this is that these systems are found to be more vulnerable to malicious code and content execution than would be expected from systems that are supposedly segregated via "air gapped" networks.

Account Management Deficiencies

Account managed deficiencies are prevalent within SCADA based systems and environments thusly increasing their potential for exploitation and negatively impacting their risk profile. SCADA environments experience many of the same issues encountered in other enterprise environments however within critical infrastructure environments, the potential impact can be observed in orders of magnitude.

- Weak passwords within privileged accounts
- Hard-coded username & password combinations (seen within documentation, binary executable and configuration system files)
- Weak and / or insufficient password protection policies

Clearly, this is again not solely unique to SCADA based environments however due to their design purpose and intent; it is outrageous and worthwhile noting.



Authentication Management Issues

Authentication management issues are also a great concern within environments where SCADA based systems are located. In many instances, little to no authentication of host-to-host communications exist thusly increasing these systems susceptibility to exploitation via attacks such as:

- Impersonation
- Replay
- Man-in-the-middle
- Etc.

Data Transmission in the Clear

Over the years auditors, assessors and security researchers have noted that data transmission is a challenge within SCADA environments. The challenge referred to here is not related to a failure at layers one through four of the OSI model but rather with layer five. It is not a failure to perform but rather a failure to implement the use of encryption. As a result, a great deal of information is transmitted in clear text within these environments in some cases traversing network boundaries from internal to external. The lack of universal adoption of encryption within these environments is troubling for several reasons all of which negatively affect the risk postures of these environments as well.

Configuration Management Issues: System Hardening & Patch Management Deficiencies

SCADA systems often suffer from a number of issues having to do with configuration management or the lack thereof. The absence of system hardening and regular, routine patching within these systems and environments encourages the frequency and commonality of services running with known vulnerabilities. Often times this occurs in the absence of reasonable rationale. Common arguments heard suggest that patching the systems and applications (which were poorly developed and coded to begin with or which are running on antiquated, non-supported operating systems) deemed critical to the utilities and environments in question, would cease to run. This is clearly not an ideal situation however one which is quite common within these environments.

Network Address Schema & Enumeration Issues

Due to a lack of ample perimeter defenses coupled with poor physical and logical architectures, issues arise within SCADA enabled environments that see them easily enumerated – from enterprise networks or in worst-case scenarios, from open external ingress points. Often address resolution protocols (DNS, ARP, etc.) are found to be exploitable within these environments via spoofing or other means. Information pertaining to system identification (OS mapping, identification and fingerprinting for example), and other information which could prove valuable to an attacker can easily be gleaned because of these deficiencies.

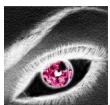
Impact of Compromise of the Water Sector on Critical Services

The environmental and health impacts of vulnerabilities to the water sector can be catastrophic in the event this critical infrastructure was targeted for a directed attack. Attacks can be carried out on the Cyber playing field and on the physical landscape. The questions we need to ask ourselves is what is the motivation in carrying out such nefarious activities? The motivation can be categorized but not limited to the following:



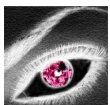
- **Insider Threat:** A disgruntled employee or officer of a company that believes he/she has been wronged by the company and commits acts that is destructive to the company. Outside individuals that have an agenda to commit nefarious activities against an organization by becoming employed or pose as an employee of the organization are also considered significant threats.
- **Unwitting Insider/Outsider:** An individual that has been unwittingly compromised via electronic means or has been emotional compromised in committing acts that are damaging to an organization.
- **Act of Cyber Terrorism:** State or Non-State sponsored activity that is targeting an organization as a vehicle to carry out objectives that instill fear, chaos and casualties based on their fundamentalist beliefs.
- **Cyber Extortion:** Organized crime or individuals acting to gain monetary advances in exchange for the control of their assets back. Nevertheless, all these can result in monetary loss, environmental disasters and even death depending on the compromise to the infrastructure.

The innovations in technology such as Web 2.0, wireless and mobile computing has helped expand and improve many IT business models. Let us take a look at mobility. Mobility for most employees can provide a lot of benefits in terms of productivity. However, in the case of critical infrastructure assets, this can increase the risk and the probability that an asset will become compromised. For example, in Harrisburg Pennsylvania a water treatment plant's cyber security was breached by an employee's infected laptop. Although nothing happened as other security counter measures compensated for the vulnerability, the absence of such mitigating solutions could have proven disastrous.



Conclusion

We have established that clean, potable water in addition to the sanctity of the infrastructure and facilities that enable its continued availability and treatment are essential, non-negotiable resources. We have also established that there are very real, very serious threats – some native to the systems and the infrastructure itself (antiquated, outdated components etc), and others being borne outside of the systems themselves, driven by third parties with malicious intent. As a result, the importance of addressing the security of these environments in a comprehensive manner is of critical importance. Assessing the physical, logical and hypothesized threats present in terms of real vulnerabilities within our drinking water and water treatment systems, is critical to our survival and the perpetuation of humanity on planet Earth. With that said US directives like DHS 2006 Sector-Specific Plan and HSPD-7 outline a proactive plan in addressing all potential surface areas (logical/physical) of protecting US critical infrastructure. However, critical infrastructure protection in other countries such as Australia is not regulated and like the US, 90% of Australia's critical infrastructure is privately owned and the protection "is shared between critical infrastructure owners and operators, the Commonwealth, and state and territory governments". We bring this fact up because critical infrastructure is global and with the rapid expansion of the Internet some are globally accessible via remote dial-up, wired/wireless misconfigurations and targeted mobile asset. As cyber security professionals and physical security professionals that work in our industry have a very big challenge in providing high assurance not only for regular business but more importantly our global critical infrastructures. If a critical infrastructure is taken out by nefarious means or act of God, it could potential affect a portion of commerce and perhaps cause wide spread panic. Stay tuned for our next release on Energy and what happens when the lights go out.



Sources:

1. UNICEF and World Health Organization (2008). Progress on Drinking Water and Sanitation. Retrieved December 29, 2009 from http://www.unicef.org/media/files/Joint_Monitoring_Report_-_17_July_2008.pdf
2. Sanctuary, M., Tropp, H., Berntell, A., Haller, L., Bartram, J., and Bos, R. (2005). Making Water A Part of Economic Development. Retrieved December 29, 2009 from http://www.who.int/water_sanitation_health/waterandmacroeconomics/en/index.html
3. <http://news.techworld.com/security/7233/water-treatment-plant-hacked/>
4. <http://www.werf.org/AM/Template.cfm?Section=Home&TEMPLATE=/CM/ContentDisplay.cfm&CONTENTID=10594><http://community.controlglobal.com/content/registration-open-9th-control-system-cyber-security-conference>
5. <http://www.swri.org/4ORG/d10/CompSys/cybersec/><http://smartgridsecurity.blogspot.com/2009/11/notes-from-2009-control-systems-cyber.html><http://news.thomasnet.com/fullstory/568259>
6. <http://www.allbusiness.com/energy-utilities/utilities-industry-water/13405895-1.html>
7. <http://www2.emersonprocess.com/en-US/news/pr/Pages/1009-OvationSecurityCenter.aspx.aspx>
8. http://books.google.com/books?id=Ja28hvTxVpWC&pg=PT106&lpg=PT106&dq=water+treatment+system+cyber+security&source=bl&ots=wy-mqt5wi3&sig=02euwc9quf42rk0r4CAe2i69x7k&hl=en&ei=fakKS6zdIM7ZnAew8rG4Cw&sa=X&oi=book_result&ct=res&resnum=2&ved=0CBkQ6AEwATgK#v=onepage&q=water%20treatment%20system%20cyber%20security&f=false
9. <http://www.wwdmag.com/New-Cyber-Security-Presentation-Added-to-WEFTEC-Safety-and-Security-Technical-Session--newsPiece16891><http://www.wired.com/threatlevel/2009/04/put-nsa-in-char/>
10. <http://news.infracritical.com/pipermail/scadasec/2009-August/004139.html>
11. http://www.semp.us/publications/biot_reader.php?BiotID=181
12. <http://cfpub.epa.gov/safewater/watersecurity/tools.cfm>
13. http://www.us-cert.gov/control_systems/csfaq.html
14. http://csrp.inl.gov/Backup_Control_Center-Documentation.html
15. <http://www.bcit.ca/news/releases/newsrelease101003662.shtml>
16. <http://ciip.wordpress.com/2009/06/21/a-list-of-reported-scada-incidents/>
17. <http://online.wsj.com/article/SB123914805204099085.html>
18. <http://www.crn.com/government/18838936;jsessionid=AQNEFBTFCSVFHQE1GHOSKHWATMY32JVN>
19. <http://washingtontechnology.com/articles/2008/04/09/water-water-everywhere-under-attack.aspx>
20. http://www.controleng.com/blog/Industrial_Cyber_Security/14629-NEERC_CIP_Compliance_and_the_Bulk_Electric_System.php
21. http://online.wsj.com/article/SB125850773065753011.html?mod=WSJ_hpp_MIDDLENexttoWhatsNewsSecond
22. <http://www.nationalterroralert.com/updates/2009/11/18/taliban-threatens-to-poison-waziristan-water-supply/>
23. <http://www.deccanherald.com/content/36652/taliban-threaten-poison-water-sources.html>
24. http://www.associatedcontent.com/article/1024560/terror_plot_poison_water_supply.html
25. [http://www.jamestown.org/single/?no_cache=1&tx_ttnews\[tt_news\]=5147](http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=5147)
26. <http://www.ionizers.org/water-terrorism.html>
27. <http://www.cdi.org/terrorism/water-pr.cfm>
28. 2002 <http://www.cdi.org/terrorism/water-pr.cfm>
29. http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection
30. Christopher, et al: *JAMA*. 1997;278(5):412-417 <http://jama.ama-assn.org/cgi/reprint/278/5/412>
31. Gold, Hal (2003). Unit 731 Testimony pp 64. Tokyo, Yenbooks.

