RISK MANAGEMENT ANALYSIS OF OUR WATER INFRASTRUCTURE'S SOFT, CHEWY CENTER

BY

MARK R. WOLFF

Master of Science

The University of Kansas

Spring, 2005

An EMGT Field Project report submitted to the Engineering Management Program and the Faculty of the Graduate School of The University of Kansas in partial fulfillment of the requirements for the degree of Master of Science.

Robert Zerwekh 3/28/05

Dr. Robert Zerwekh Date

Committee Chair

Tom H Bowlin 3/28/05

Dr. Tom Bowlin Date

3/28/05

Ms. Annette Tetmeyer Date

3/28/05

Herbert Tuttle Date

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I must first and foremost thank my lovely fiancé Marthe whom has been a source of constant support and encouragement. She has always understood when I had to cancel or postpone time to spend with her in order to complete coursework. I can't wait to start our new life together.

I would also like to thank David Shultz, a recent Engineering Management graduate. David has been a close, long-time friend and encouraged me to start the Engineering Management program. David and I were able to schedule several classes together which made them that much more enjoyable.

I must also acknowledge my employer, Burns & McDonnell for both their moral and financial support of my education. I would not have done it without either.

Finally, I would like to thank all of the wonderful faculty and staff of the Engineering Management program. All of whom are genuinely interested in the professional and personal enhancement of students in the program. This is why the program is growing successfully. I believe this program has better prepared me for my current career path, and frankly, given me insight and training for future careers.

Thank You.

MARK R. WOLFF

Executive Summary

National security has become a growing concern since the terrorist attacks on the United States in September of 2001. A safe public drinking water supply has undoubtedly always been considered a priority nationwide. Now, more than ever, national security is merging with safe drinking water creating a need for increased awareness, better technology and new kinds of training. This merger has also spawned a new market in the engineering and technology industry.

The process by which this country's water infrastructure is designed, constructed and managed is changing. More fencing, better alarm systems and high-tech cameras will be a part of this change in thinking. These physical security features may be considered the "hard outer shell" that secure a water supply system from intrusion and malevolent threats. However, once a fence is cut or a camera breaks down, it will be the "soft insides" of the system that are left to defend critical infrastructure. The "soft insides" include management of policies, procedures and people that are relied upon for effective security of facilities and operations within the overall system. Practically allocating resources to the correct places at specific water infrastructure will help to meet security goals.

The challenge for the future is to refine security measures at water systems without waiting to learn from future terrorist acts.

I. Introduction

The United States has the safest drinking water and lowest rates of waterborne diseases in the world (States, 2003). This statistic is the result of high water quality standards, available technology that can meet those standards and trained professionals who take pride in the valuable service they provide. Most citizens only see the end result: clean, safe, potable water from the tap.

The design of water treatment plants and systems has always included some level of safety and security. Simple locks on doors, alarms that sense tank overflow levels and enclosures over open water basins have been standard features. Fences, area lighting and cameras have been included among typical security measures. These have typically been in place to prevent accidents or minor theft and vandalism.

Now more, and smaller, water systems are beginning to resemble maximum security prisons rather than water treatment plants. Facilities are installing motion detectors, razor wire and tamper-proof locks. Shatter-proof glass, vehicle barricades and full-time security personnel are becoming common features. Is all of this the result of carefully planned risk management or unrealistic terrorist fears?

Managing risk at critical infrastructure by managing physical security components, policies and personnel can be a difficult and abstract task and requires the answering of the following questions:

- What are the critical assets within the system?
- What assets are the most vulnerable?

- What is the most realistic, credible threat to the system?
- How effective are the current security measures protecting the most critical assets?
- How is risk quantified?
- How are resources and money best allocated?

This paper will examine issues that will assist public drinking water utilities in answering these questions and make educated decisions regarding risk management. This study will begin to explore what is currently being done to secure critical water infrastructure, its effectiveness and whether it is enough, or too little. As risk management becomes a growing issue at water utilities, the usefulness of the information discussed in this paper will apply to emerging markets in the engineering consulting industry.

II. Historical Risk Management

Although recently more attention has been given to this topic, the concept of risk and security management at water infrastructure is not a new one. Whether the intentions were to minimize effects of drought, floods or terrorists, some level of risk management has been designed into every water system. This section will briefly describe the regulatory and historical events that have led the industry to where it is today in regards to security management.

a. Regulatory Events

Efforts to protect the nation's water supply actually began long before the events of September 11, 2001. The President's Commission on Critical Infrastructure (PCCIP) was formed in 1996 to study all forms of the nation's infrastructure in an effort to determine the numerous associated risks. The Commission concluded that the nation's water systems are highly vulnerable to threats and attacks. In May 1998, President Clinton signed Presidential Directive 63 which identified drinking water as one of America's critical infrastructures. The National Security Council decided that the Federal Environmental Protection Agency (EPA) should be responsible for developing a process to study community water supplies and develop a method to assess their vulnerability. In November of 2000, EPA partnered with the American Water Works Association Research Foundation (AWWARF) to provide funding to engage the services of Sandia National Laboratories to assist in the effort. Sandia is the Department of Energy's lead laboratory for physical security research and development. Sandia has developed

security and risk assessment processes for nuclear weapon facilities, international training courses, federal dams, information operations and other high consequence facilities. A methodology for water infrastructure was in development on September 11, 2001. As a result of these events, Sandia expedited the completion of their methodology, referred to as the Risk Assessment Methodology for Water (RAM-W).

On June 12, 2002, President Bush signed the Public Health Security and Bioterrorism Preparedness and Response Act (Bioterrorism Act) into law. The Bioterrorism Act is regulated by the EPA and required all community water systems serving over 3,300 people to conduct an assessment of vulnerability and to update or develop an emergency response plan. As part of the Bioterrorism Act, all public drinking water utilities must have completed their vulnerability assessments by June 2004. The new law also outlined funding to assist agencies in the preparation of such plans.

b. Historical Incidents

Risk and security management in the water supply industry is nothing new. Risk assessments and security measures have long been in place at water supply facilities, especially dams. This is mostly due to the devastation that can occur when dams fail. Notably, in 1976, 14 people died and millions of dollars in property was damaged when the Teton Dam in Idaho failed (Lowery, 2003). Several other large dam failures in the early 20th century took thousands of lives. There have been fewer and fewer dam disasters in recent years, indicating that what

has been learned from past incidents has improved safety. There has never been a major act of terrorism on the U.S. water supply. The industry is now attempting to be proactive in security countermeasures to avoid having to learn from potentially catastrophic events.

In the past, there have been a handful of incidents that have tested the public confidence in the country's water supply systems. Most recently, in 1993, nearly 400,000 people in the Milwaukee, Wisconsin area became ill when cryptosporidium was present in the water supply.

Following September 11th, the United States as a whole has increasingly considered intentional acts of terrorism as a realistic threat. This threat may come in many forms, including through use of our own systems and equipment against us.

In the few years since September 11th, several events have taken place that have put more emphasis on protecting water supplies against malevolent attacks. In April 2002, an attempt to sabotage the water supply to the United States Embassy in Rome, Italy with the deadly toxin ricin was foiled. In August 2003, a widespread power blackout in the eastern U.S. (not the result of terrorism) exposed vulnerabilities at several large metropolitan water works. The blackout identified aged back-up systems at major metropolitan water systems and plant operators' inability to run facilities manually. Numerous other specific threats and reports of suspicious activities at and near water supply facilities have been warning flags that the battle is no longer just against the neighborhood vandal and disgruntled employees.

Public water systems have traditionally been a source of civic pride and education. Besides their obvious function for the public good water treatment plant is often showcased as an example of how the public's money is spent to improve the quality of life by supplying clean, safe water. It can be a very visual example that is easy to understand. Just a few short years ago when water departments were so proud of the enormity and efficiency of their water systems that they invited foreign dignitaries and any other interested parties to visit water treatment plants. Engineers would happily explain entire systems and how they worked. Since September 11th, water systems have been much more cautious with system information and public tours.

III. Risk Management of Water Systems

Risk management is a concept that is commonly seen in the business environment and project management. It involves managing anything that may happen that could create an adverse effect on a project's schedule, cost, quality or scope. The basic principles of managing risk can be applied to management of water supply facilities and can be broken into these three steps:

1) Identifying Risks and Threats
2) Quantifying an Prioritizing Risk
3) Mitigation and Contingency

This section of the paper will detail each of these steps that are applied at water infrastructure facilities, following a discussion of the importance and role of risk management.

a. Role of Risk Management

Managing risk at water treatment facilities is important for several reasons besides to achieve the ultimate goal of providing safe, potable and reliable water to the public. Water infrastructure is closely linked to other infrastructure, including hydroelectric power, transportation and wastewater. The chemicals used in water treatment are a major component of certain markets in the chemical industry. Although this paper will discuss only public water supply facilities in general, many of the risk management principles apply to other infrastructure. This point is nothing new. In 1941, FBI Director J. Edgar Hoover wrote, "It has long been

recognized that among public utilities, water supply facilities offer a particularly vulnerable point of attack to the foreign agent, due to the strategic position they occupy in keeping the wheels of industry turning and in preserving the health and morale of the American populace." (Copeland, 2002).

Risk management is intertwined with many other facets of management at a drinking water facility that can all be tied to security. Figure III-1 illustrates this relationship.

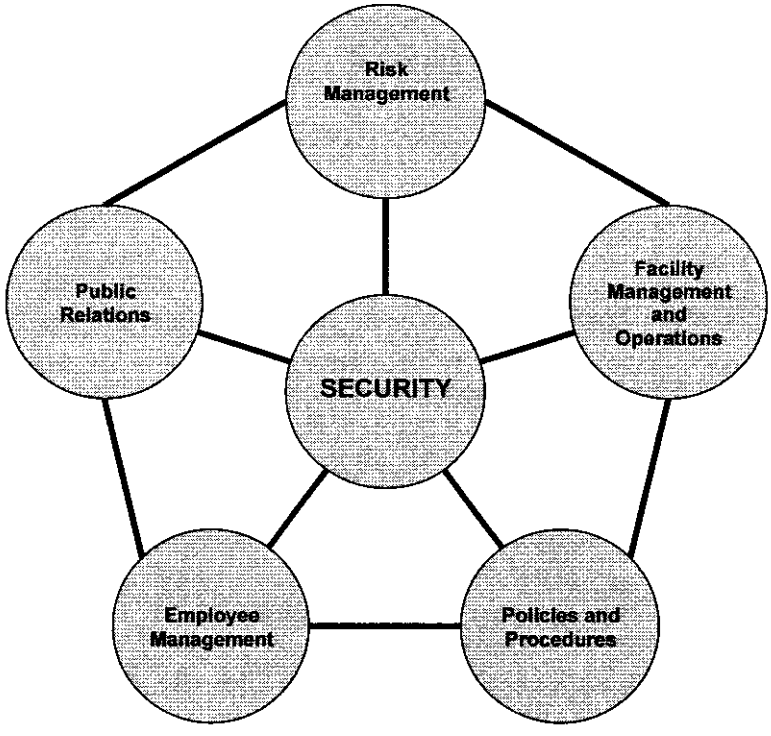

Figure III-1.

Security should be at the center of every function at a water facility, some more than others, based on their criticality to the entire system. Larger systems serving

larger populations will typically have more resources to devote to security. Larger systems also have more reason to emphasize security due to greater risks.

b. Identifying Risks and Threats

The assessment of risk and vulnerabilities is the first and most important step to understanding what risk management needs exist. Vulnerability assessments are designed to help drinking water utilities evaluate their susceptibility to terrorism or other intentional acts that could disrupt the water supply and identify actions that reduce or mitigate risk (Journal AWWA, 2003). These assessments mandate that systems examine and consider risks involving all components of the water system. This is something to which many smaller-sized systems had never given much thought or any additional resources.

The methodology to complete vulnerability assessments requires that systems identify a design basis threat against which the existing system and proposed security can be evaluated. Several types of threats should be considered including an insider, outsider, combinations of the two and a "cyber" threat. Systems have discovered that their most realistic, credible threat is often their own water plant operator. This is a person who has full knowledge of the system and most likely full access to the system. Once the adversary is known, it can be determined how and to what level to protect.

Government and private utilities have given increased thought to the possibility of weapons of mass destruction. This potential threat applies to all type of

infrastructure including our airports, power generation facilities, dams, bridges and water supply. Hazards of threats to water and other infrastructure include loss of power and communications, explosions, chlorine releases, broken water mains, pump failure, storage tower failure and biological and chemical contamination. Economic damage may be just as much an objective of an attack as injury and death.

c. Quantifying and Prioritizing Risk

Determining which risks to ignore and which to manage may be the most difficult task in risk management. Assigning quantitative values to these factors and calculating risk values can be done a number of ways. Essentially, an event or threat with high probability and high consequences is a much greater threat than a threat with a low likelihood of occurrence and minimal consequences. Determining which risks are the greatest and assigning priorities based on those determinations will allow a water system to most effectively assign resources. Prioritization of risks should be based on factors such as likelihood of occurrence, potential consequences and the system's effectiveness at preventing an undesirable event.

Consequences of a malevolent attack on a water system must be evaluated and prioritized based on public perception as well. If the public's confidence is low in the safety of their drinking water, this can damage the utility. This may be the result of a real or perceived incident or even of journalistic misrepresentation.

d. Mitigation and Contingency

Developing contingency plans to deal with the most critical risks and mitigate their consequences is the final step. Security systems and policies must be analyzed for their effectiveness to mitigate risks at water supply facilities. This analysis should be based on the ability to detect, delay and respond to a threat.

Detection as a function of a security system is the discovery of an adversary action. A related function during the detection phase is confirmation that the concern or alert is valid. For instance, a door sensor alarm relayed back to a radio system does not represent a valid adversary until it can be confirmed by some other means that the "door open" indication was an intrusion by an unauthorized party. Confirmation can occur by any independent means such as visual affirmation, closed circuit television, keypad confirmation or other methods that validate the intrusion.

A well-designed system will delay or impede the progress of the intruder from committing their act. Physical features such as walls, fences and doors achieve passive delay. Features that are activated by sensors or remote controls in response to the intrusion achieve active delay.

The third function consists of interrupting or stopping the adversary, and is referred to as response. The time to achieve response is crucial to maintaining security effectiveness. An effective security system must be able to detect the adversary

early and delay them long enough for the response to arrive and stop them before their mission is accomplished.

Designing a water system with multiple paths and contingency sources is often a way to mitigate risk. Purchasing spare equipment and storing it in a secure, off-site location can minimize long down times during unplanned failures. These methods can often be expensive and may need to be implemented early in the design of the system if retrofitting and working around existing structures is difficult.

e. Legal Issues

Emergency Response Plans (ERP) and vulnerability assessments developed for a water system will contain sensitive, confidential information. This includes information that is specific to a water system and describes points of vulnerability and emergency operations. This information can easily serve as a road map to the weak spots and "low-hanging fruit" within a water system. There are local and state freedom-of-information laws, or "sunshine laws", that give the public full access to sensitive documents controlled by public entities. Since September 11, 2001, dozens of state legislatures have passed exceptions to their freedom-of-information laws in the name of homeland security. These exemptions allow emergency and evacuation plans to be kept secret and block out maps of government buildings, utility plants, bridges, water and wastewater lines and transportation routes (Locy, 2004).

Recently, with the help of the American Water Works Association (AWWA), states have begun to more aggressively counter efforts by the public to access documents that may pose a threat to critical water infrastructure. The AWWA, in particular, has urged public utilities to lobby for protection of vulnerability assessments under these laws. More and more states are amending their laws to ensure that vulnerability assessments will not be subject to disclosure (AWWA, 2004). This movement is an important, and controversial, issue to determine what the public has a right to see and what information has the potential to compromise the security of a facility.

Another legal issue with facility security is the ability to effectively prosecute trespassers, vandals and others. Posting NO TRESPASSING signage on buildings and fences is a very effective tool in prosecution. Video cameras can not only help with operations and detecting events, they can be used in court to prosecute individuals who violate the law.

In recent years, public utilities have begun paying closer attention to school tours. Subtle measures may be taken such as having all tour groups sign a visitor's log. Sometimes tours are gathered for a group photo, not only as a souvenir for the visitors, but for the facility to document all who were present. Tour groups are restricted to certain areas of the facility, watched by surveillance cameras and asked not to take photographs or video.

IV. Risk Management Strategies

The trend toward securing our country's water infrastructure with physical security can be compared to the hard, outer shell of a piece of candy. Physical security measures such as fences, barricades and alarms are all good, reliable resources and are necessary for protection. However, these security tools should not be relied upon as the sole source of protection. Once past the initial alarms, lights, and barricades, the "soft, chewy center" of infrastructure is made up of the management of policies, procedures, emergency manuals and people. These are the people who actively review, update, train from, implement and maintain the security features and procedures. Ignoring important aspects of security and risk management gives a false perception of security and make a facility an easy target for a perceptive adversary.

This section will address some common "hard" security features and the "softer" insides that must be developed and maintained to effectively detect, delay and respond to threats at water utilities. Some weaknesses and shortcomings of certain parts of these features in water infrastructure management will be part of this discussion. Proposed strategies to deal with these issues and long term impacts of a security emphasis will also be presented.

a. The Hard, Outer Shell

When one thinks of security, locks, fences, alarms and guards usually come to mind. These can all be critical to securing a public drinking water facility and play an important role in addressing vulnerabilities. Now more than ever, cyber security