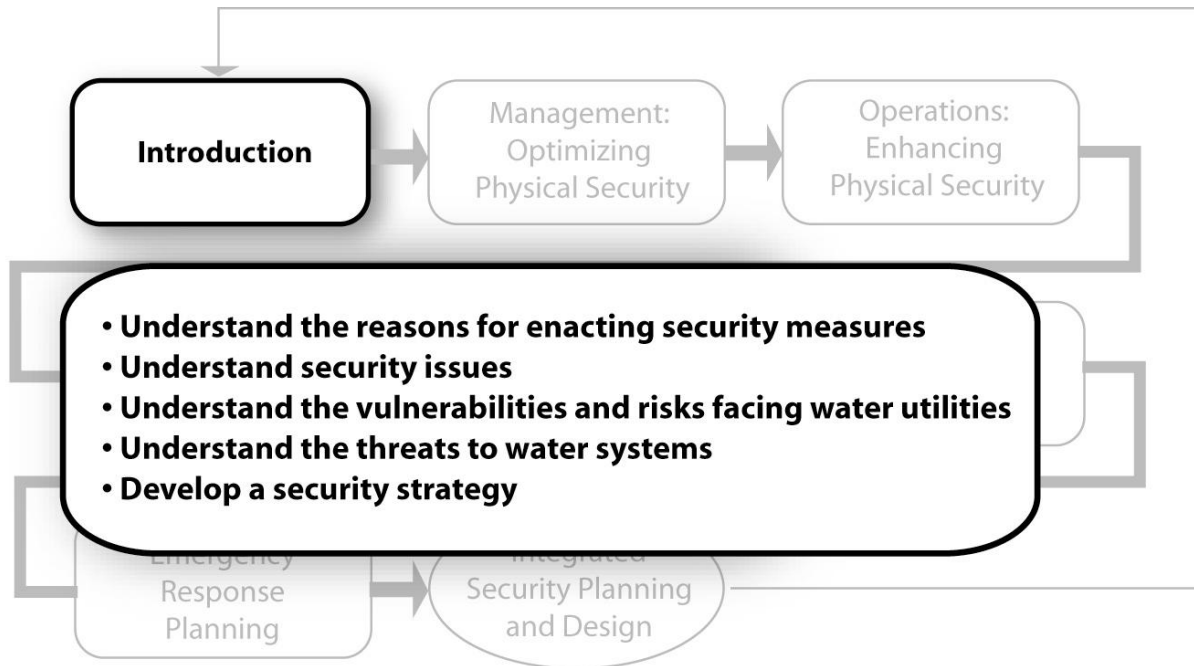


Introduction



1.1 Overview

Improving the physical security of water systems in the United States has become a priority for utility managers and governing bodies since the events of September 11, 2001. Protection of water systems from malevolent acts is also a very high priority for federal agencies such as the Department of Homeland Security (DHS) and the U.S. Environmental Protection Agency (EPA). In 1998, Presidential Directive 63 designated water systems as part of the nation’s critical infrastructure. For water utilities, however, enhancing physical security is just one of many priorities. Because of this competition for limited resources, including personnel and financial, the security tactic that a utility takes needs to be carefully thought out, applying a balanced approach including each of the three major areas available to the utility manager: 1) management tools, 2) operational approaches, and 3) physical security design features

Numerous other documents, guidance manuals, and standards of operations focus on the first two areas. The purpose of this American Water Works Association (AWWA) Security Guidance is to provide water utilities with a document that also includes physical security design options and how they can be tailored to individual water systems. Because these three areas are not mutually exclusive, but are in fact integrated and interdependent, this document incorporates all three. The diagram in Figure 1-1 illustrates these interrelationships to assist in understanding the underlying intent of this document.

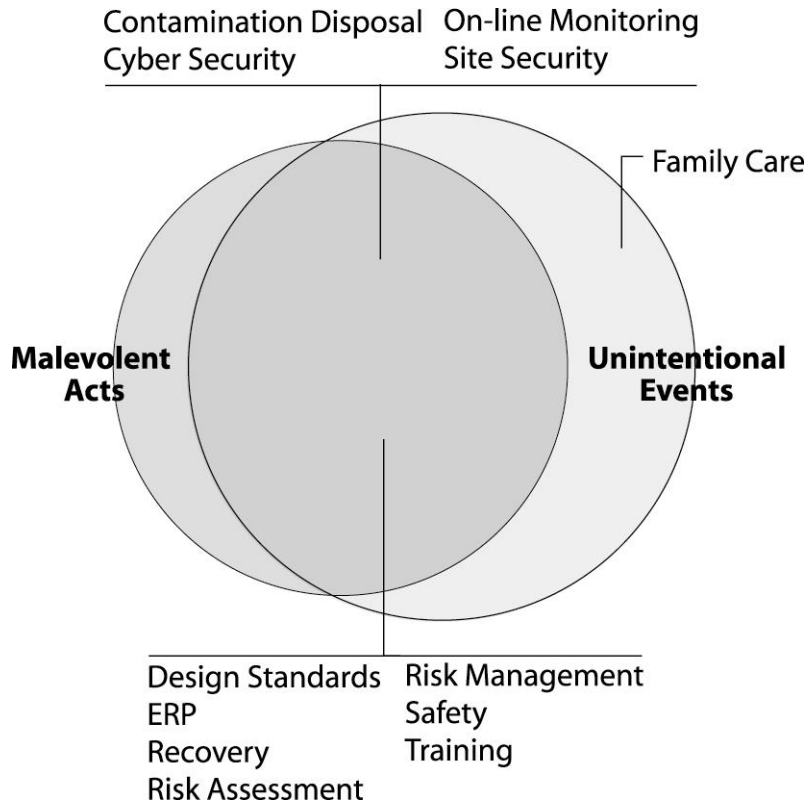


FIGURE 1-1
Interrelationships Between Common Utility Programs and the Reduction of Risk

This document provides guidance and a framework from which management, operations, and design of a water system can be conducted to improve the security of the system. Additional information that addresses threat mitigation, as well as general information on Homeland Security that may be useful to water professionals, is provided in the annotated bibliography.

This section begins with the background and processes used to identify the priorities for the physical security protection of a water system. Through vulnerability and risk assessment, utilities will identify the level of threat that will drive development of a security strategy.

1.2 Reasons for Water Utilities to Enact Security Measures

There are a number of reasons that a utility would invest in the security of its system and facilities, including meeting the goals defined in the utility’s mission statement and regulatory and legal requirements, among others. Investments can also serve the dual purpose of protecting the water system from both malevolent and natural acts. For example, whether a pump station is disabled by a criminal or a hurricane, it is in the water utility’s best interest to have a plan that reduces the impact of either event.

1.2.1 Mission Statement

The purpose of a water utility is articulated by its mission statement and further defined by its goals and priorities. These mission statements have at their core the protection of public health and safety due to water quality or reliability attacks on the public water system. Many utilities recognize that their mission statement includes the need to:

- Provide high quality water in sufficient quantity to its customers
- Operate in a manner that protects against, detects, and responds to man-made threats and natural disasters from both inside and outside the utility
- Provide a safe work environment for employees and safe, reliable water delivery for the public
- Identify and maintain assets that are critical to the utility's ability to meet its mission

To meet these goals, a utility can identify and take the measures necessary to reduce its risk in the face of malevolent acts.

1.2.2 Regulatory and Legal Requirements

Regulatory and legal reasons are also motivations for water utilities to make security improvements, including best practices or lessons learned considerations.

1.2.2.1 Regulatory Drivers

Public Health Security and Bioterrorism Preparedness and Response Act. In June 2002, Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act (PL 107-188), which requires vulnerability assessments be performed and Emergency Response Plans (ERPs) be created or updated for community drinking water systems that serve more than 3,300 people. There could, in the future, be pressure from groups inside and outside of the government to make mandatory the implementation of recommendations resulting from the assessments.

Chemical Security Act. As of this writing, there is pending legislation that could require water systems to address the security of certain chemicals. The Chemical Security Act of 2003 (House of Representatives Bill 1861 and a similar Senate Bill [SB 157]) direct the EPA to regulate facilities that store certain toxic chemicals over a specified threshold amount. The act would require the facilities to assess the vulnerability of a water source to an attack or other unauthorized release; to identify hazards that may result from such a release; and to prepare a prevention, preparedness, and response plan. Facilities that store chlorine in quantities over 2,500 pounds would be subject to the Chemical Security Act as it is currently drafted. However, the legislation may use the chemical lists and thresholds established by the Risk Management Programs (40 CFR Part 68) to determine applicability.

1.2.2.2 Legal and Liability Issues

A basic tenet of legal liability may compel a water utility that is made aware of a condition to take reasonable steps to eliminate or mitigate a hazardous condition. Publications such as this one that discuss the need for water utility security, and the materials published by EPA and other entities, could be considered notice that a hazardous condition may potentially exist. Once a vulnerability assessment is complete, the resulting recommendations also could be considered as notice of a dangerous condition. This notice could potentially result in liability if the recommendations are not addressed. In some cases, water utilities may be able to claim immunity based on their charters or municipal laws; however, some state laws waive or limit this immunity. A finding of negligence for damages stemming from a security breach generally would require:

- Knowledge or reasonable ability to foresee the damages
- A duty to the injured person
- Violation of the duty proximately causing the injury

Generalized warnings of terrorism against water utilities may not impact liability, but a warning relating to a specific plant or location could. The paraphrased axiom that, “the best defense is a well thought out and implemented security program,” can be applied here. Court rulings have found that a water utility must exercise reasonable care in operating and maintaining its system. The definition of “reasonable care” is key in determining liability. As more water utilities implement security improvements, it could be argued that the definition of reasonable care is evolving to include installation of security systems that only a short time ago were rarely found in water systems. This document will include a two-tiered approach to security-related improvements using Basic and Advanced categories. A water utility can identify those measures that actually provide security improvements and that are a balance of the available resources, the utility’s ability to execute the improvements, and ongoing operational aspects of the utility.

The Basic category is a reasonable care approach to reduce identified risk levels at the most critical assets. The Advanced category adds Best Business Practices to further lower risk levels across the water utility, but at increased resource expenditures.

Benchmarking the security-related improvements that utilities have made can help define a standard and provide guidance for other utilities struggling to determine which improvements to implement. Utility staff can evaluate common practices in the water industry as one approach to making decisions regarding the appropriate level of protection and investment for their systems.

1.2.3 Other Reasons

Other reasons that water utilities have cited for the implementation of security systems include:

- Providing protection against non-terrorism threats such as vandals, low-level criminals, and disgruntled employees. Vandalism and theft are a problem for many utilities, especially those in larger urban areas – one that installing security systems can help to mitigate or prevent.
- Protecting employees from outsiders entering plants.
- Providing operational benefits beyond heightened security. For example, installing backup generators to provide power in the event of an attack on the power substation feed will also provide mitigation for power outages caused by other events, such as natural disasters or construction-related incidents. Similarly, as part of vulnerability assessments, utilities that add redundant pumps for pumping systems would significantly reduce process-related consequences if the main pumps are no longer operational.
- Assuming the responsibility to maintain public confidence in the water system and provide service to the community.

1.3 Overview of Water System Security Issues

Interruption of water system service, whether from natural disasters or malevolent actions, can result in widespread public health impacts and economic or environmental damages. Because water systems have been identified as critical infrastructure, these systems may be a target for adversaries. Some examples on how water systems could be attacked by adversaries are listed below and summarized in Table 1-1:

- Introduction of volatile compounds to the raw water system, which can cause explosions and shut down water treatment processes
- Large releases of chlorine gas from water treatment facilities or booster disinfection facilities to cause injury and death to workers and public within and outside of the facility
- Physical destruction of the water system assets
- Introduction of toxic chemicals or biological contaminants to the water treatment, storage, and distribution systems
- Water distribution systems used to transport chemical and biological contaminants to a major or critical water customer

Misuse of the Supervisory Control and Data Acquisition (SCADA) or connected cyber systems, which can cause chemical over- or under-dosing, system interruptions, and damage to the drinking water system components.

TABLE 1-1
Threats to Water Systems

System	Overall Issue	Examples of Potential Threats	Impacts to		
			Facilities	Personnel	Community
Source Water and Water Treatment Facilities	Source water and delivery areas are sometimes remote, not typically secured other than by a fence	Damage to or disabling of critical assets Toxins introduced into source or treatment plant Release of chlorine gas	Damage to structures and equipment Significant disruption to treatment processes	Direct, potentially fatal injuries to workers from explosives or toxic substances	Disruption of service Adverse health effects from contaminated water or chlorine gas plume
Distribution Systems	Numerous facilities and piping are easily accessible and are largely unmonitored	Use of system as a “conduit” for adversaries Improvised explosive device set in facilities or placed in vaults	Damage to piping and storage tanks	Direct, potentially fatal injuries to workers from explosives or toxic substances	Disruption of service Adverse health effects from using contaminated water Damage to surrounding buildings and inhabitants
Pump Stations	Some locations are remote and unmanned	Individuals driving or walking up to a facility to damage or disable equipment Shooting at pump station panels	Damage to structures and equipment	Direct, potentially fatal injuries to workers from explosives or toxic substances	Adverse health effects from lack of water or contaminated water
SCADA System	Hacking the SCADA system through Internet or interruption of radio frequencies	Disabling of alarms Taking control of flow and processes Preventing operators from knowing what is occurring	Significant disruption to treatment and distribution processes	Indirect effects from being unaware of conditions	Disruption of service Adverse health effects or lack of access to account information

1.4 Vulnerability and Risk Assessment

The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 has required that all community drinking water systems serving populations greater than 3,300 conduct a vulnerability assessment (VA). The VAs have helped utilities to understand the most likely threats, the most critical facilities and assets, and the relative risk for those critical facilities and assets. The results of the VA provide a framework for the utility to enhance the physical security of its water system so that its mission may be achieved.

1.4.1 Definition of Vulnerability

As defined in the Sandia National Laboratories' RAM-W™ approach, "vulnerability" is an exploitable security weakness or deficiency at a facility. Further definitions of vulnerability include these:

- A characteristic of a critical infrastructure's design, management, or operation that renders the infrastructure susceptible to destruction or incapacitation by a threat.
- A flaw in security procedures, software, internal system controls, or operation that may affect the integrity, confidentiality, accountability, and/or availability of data or services. Vulnerabilities include flaws that may be deliberately exploited and those that may cause failure due to inadvertent human actions or natural disasters.
- Any weakness that can be exploited by an aggressor or, in a non-adversarial threat environment, that can make an asset susceptible to hazard damage.

1.4.2 Definition of Risk

As defined in the Sandia National Laboratories' RAM-W™ approach, "risk" has two components: 1) a measure of the potential damage to or loss of an asset and 2) the probability of an undesirable occurrence to that asset. Further definitions of risk include these:

- The potential for realization of unwanted, adverse consequences to human life, health, property, or the environment.
- The quantitative or qualitative expression of possible loss that considers the probability of a hazard causing harm together with the consequences of that event.

Risk is usually expressed as a function of the probability of the occurrence of an adverse effect and the consequence of the affect on the ability to maintain function.

1.4.3 Objectives

The objectives of vulnerability and risk assessments are to:

- Identify threats to the water system assets, including infrastructure, quality of water, employees, information, finances, etc.
- Identify the specific assets that may be impacted by the identified threats, and the relative criticality of these assets.
- Determine the likelihood that a threat may materialize.
- Calculate the consequences of losing part or all of the water system assets.
- Evaluate existing countermeasures.
- Analyze current risks associated with threats and assets.
- Identify additional countermeasures and prioritize based on a risk-reduction analysis.

The goals of the vulnerability assessments are to develop information that the utility could use to:

- Protect public health and safety
- Protect or ensure the supply of water
- Provide a secure workplace for employees
- Protect the facilities the identified Design Basis Threat (DBT)
- Provide security management practices
- Provide measures to minimize insider threat
- Protect computer access and data, communications, and SCADA
- Protect operational systems and building support systems
- Protect power supplies and emergency backup power

1.4.4 Vulnerability Assessment Methodologies

Several methodologies can be used to conduct a VA. The assessment itself is important, not necessarily the specific method used. As long as the assessment is accurate for a utility's own particular given risks, then any method that produces an accurate picture of vulnerability and risk is acceptable. The two most common methods are:

- Risk Assessment Methodology for Water Utilities (RAM-W™) developed by Sandia National Laboratories with funding from EPA.
- Vulnerability Self-Assessment Tool (VSAT™) developed by Association of Metropolitan Sewerage Agencies (AMSA) with EPA funding.

Other methods that can be used to conduct and vulnerability and risk assessment include, but are not limited to:

- Security Vulnerability Self Assessment Guide for Small Drinking Water Systems (May 30, 2002) by the Association of State Drinking Water Administrators (ASDWA) and National Rural Water Association (NRWA) for populations less than 3,300.
- Security Vulnerability Self Assessment Guide for Small Drinking Water Systems Serving Populations between 3,300 and 10,000 (November 13, 2002) by ASDWA and NRWA.
- The application of CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability), a method used by the military to assess the attractiveness of a particular target.

Use of a hybrid model is acceptable if it establishes vulnerabilities and risks.

1.4.4.1 Risk Assessment Methodology for Water Utilities (RAM-W™)

The RAM-W™ methodology, illustrated in Figure 1-2, is a “consequence-driven” approach that focuses on evaluating the effectiveness of a security protection system (Sandia Corporation 2002). As such, it offers numerous benefits. First and foremost, it offers utilities a systematic, defensible approach to security protection systems. RAM-W™ helps utilities to identify those system

components that are critical for the system to function and, in turn, helps them to prioritize security upgrades and/or modify policies and operational procedures to mitigate identified risks. In turn, it offers utilities a way to develop balanced security protection systems so that they can allocate the appropriate resources to the areas where they are most needed to reduce risk.

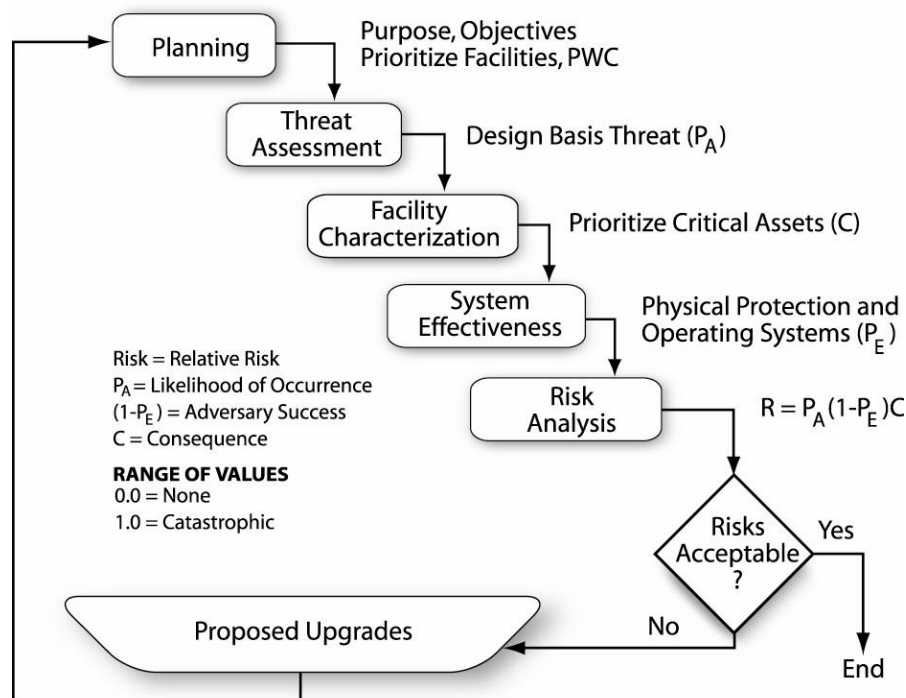


FIGURE 1-2
RAM-W™ Methodology

1.4.4.2 Vulnerability Self-Assessment Tool (VSAT™)

VSAT™, shown in Figure 1-3, is a software-based tool for risk-based and cost-managed security evaluation and planning. It is specifically designed to assist utilities in addressing the tasks necessary to complete the six basic elements that the EPA requires for a water system vulnerability analysis. VSAT™ imposes the rigor and logic necessary to perform an assessment that results in a comprehensive analysis and that addresses these utility asset categories: 1) physical, 2) information technology, 3) knowledge, 4) people/employees, and 5) customers/finances. A description of the water system should be developed for each category to aid the utility in interpreting the results of the assessment provided by the VSAT™. Additionally, the utility should review, and modify as applicable, the software-generated language to ensure that the language is specific to the water system being assessed. More information about VSAT™ can be found at www.vsatusers.net.

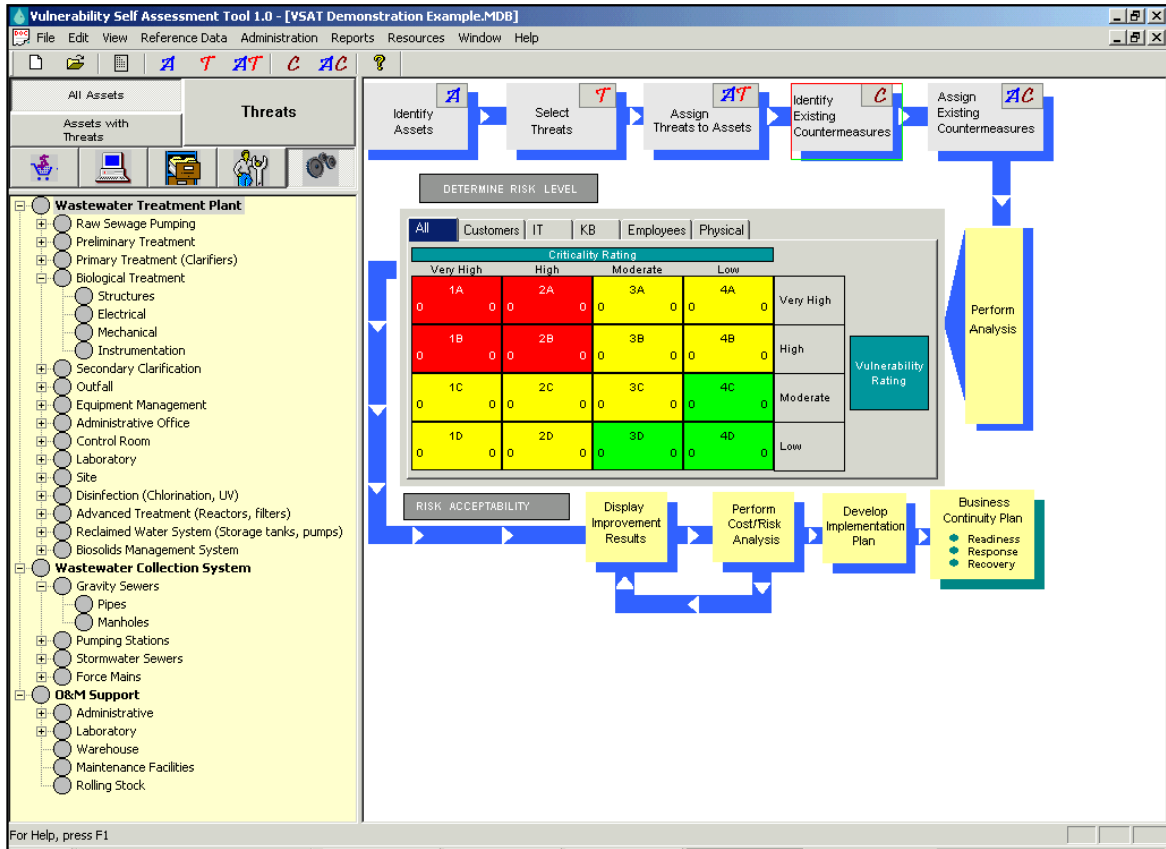


FIGURE 1-3
Vulnerability Self-Assessment Tool (VSAT™)

1.5 Understanding the Threats to Water Systems Before Developing a Security Strategy

Threats to water systems have always included natural disasters, recurring events such as extreme weather (e.g., flooding, lightning), and accidental (human-caused) events (e.g., chemical spills, vehicle collision). Identified concerns for utilities from malevolent acts, such as vandalism, criminal activity, and terrorism, exist. The use of water as a weapon, a means to defeat an enemy, or to affect a population has historical precedent (see www.worldwater.org/conflict.htm).

The events of September 11, 2001 have heightened the way that utilities think about these malevolent threats. Now, privately and publicly owned water utilities, along with other public infrastructure and essential service providers, are clearly potential targets for destruction and disruption from domestic and international adversaries. This concern has alerted water industry leaders, causing them to recognize and address the potential consequences of threats such as vandalism and employee misconduct to enhance their ability to maintain business continuity during these types of events.

1.5.1 Malevolent Acts

Deliberate, malevolent events are intended to affect as many people as possible in order to create concerns among the public and promote distrust of the authorities. This, in turn, causes dissention and division and makes it easier for adversaries to affect the political and economic well-being of the community.

1.5.1.1 Types of Malevolent Acts and Adversaries

Physical attacks on raw water supplies, water treatment plants, and distribution systems can take different forms, creating a variety of results. The bombing of critical treatment plant processes or a pump station, for instance, would result in significant property damage. Similarly, destruction of electrical power grids or chemical suppliers servicing a water treatment plant would significantly reduce or halt water deliveries for an indefinite period of time.

Sabotage or physical damage to a utility's chemical inventory would cause consequences for plant staff, emergency response personnel, and community within the zone of influence. Once the initial consequences of such an attack are addressed, the secondary concern would be the facility's inability to use that chemical until temporary measures are established or the system is repaired.

Other types of malevolent acts include:

- Physical damage and destruction to the infrastructure assets
 - Use of explosive devices
 - Arson
 - Introduction of a flammable liquid into the water system
 - Vandalism
 - Sabotage of valves, tanks, etc.
 - Introduction of a chemical agent that can permanently contaminate the interior of pipes and storage tanks
 - Damage to the power supply
 - Destruction of vital infrastructure
- Disruption of the water system
 - Introduction of a toxin into the source water, treatment facility, or distribution system
 - Hacking into the SCADA system
 - Removing hardcopy files or deleting electronic files
 - Vandalism
 - Sabotage of valves, tanks, etc.
 - Interrupt operations supporting the public
- Harming the workers and public
 - Release of toxic substance (e.g., chlorine)
 - Personal assault with or without a weapon on employees
 - Use of explosive devices

introduction

- Arson
- Kill, injure, or affect the health of large numbers of people
- Use of facilities for other malicious purposes
 - Access of customers' financial information
 - Equipment theft for personal gain
 - Threat of contamination to invoke public fear

There are numerous types of adversaries as shown in Figure 1-4. Threats may originate from an "insider" or from an "outsider." An insider is a person with knowledge of the water utility and who has access to the facilities or portions of the system as part of his or her daily work activities. Insiders typically have access to information systems as well. The appearance of an insider at a utility facility does not typically cause suspicion. Examples of insiders include employees, vendors delivering materials, and onsite contractors.

An outsider is a person who is not normally allowed access to any of the water facilities. Suspicions might be raised if such a person is seen on utility property. Outsiders typically do not have access rights to buildings or information systems. Some outsiders, however, can have insider knowledge. These outsiders can include former employees, contractors, or consultants who have some access or knowledge of the facility.

One way of differentiating these two is the manner of mitigation. For an insider, a utility is able to apply insider risk reduction measures. The individuals need to fall under the utility's personnel policies, procedures, and control. If they do not, the only remaining methods that can be applied are those specific to an outsider.

The spectrum of malevolent acts is broad, and the actions to mitigate the risks associated with these threats are more of a continuum than a discrete number of countermeasures. Consequently, specifically in Section 2, "Management Considerations for Optimizing Physical Security," and to some extent in Sections 3 and 4, "Operational Considerations for Enhancing Physical Security" and "Design Considerations for Developing Physical Security at New Facilities and Retrofits," respectively, risk reduction actions are presented in the context of defined levels of threats.

In the sections that follow, threat levels are assumed to have the following defining characteristics as shown in Table 1-2.

Prior to choosing a threat level on which to base a design, make operational changes, or revise management policies, it is imperative to perform a vulnerability assessment and risk analysis on the existing (or planned) water system. A thorough vulnerability assessment performed using either RAM-W™ or VSAT™ (see Section 1.4.4, "Vulnerability Assessment Methodologies") will identify the threats that should be addressed; a subsequent risk analysis will provide decision makers with the data required to choose a strategy to reduce risks in the design, management, and operations of the water system.

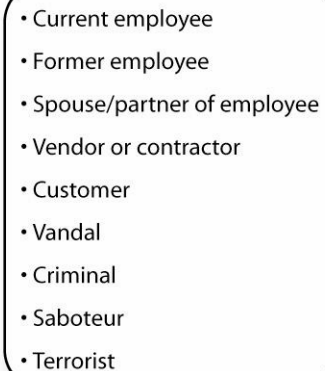
- 
- Current employee
 - Former employee
 - Spouse/partner of employee
 - Vendor or contractor
 - Customer
 - Vandal
 - Criminal
 - Saboteur
 - Terrorist

FIGURE 1-4
Examples of Adversaries

TABLE 1-2
Threat Level Characteristics

		Threat Level			
		Vandal	Criminal	Saboteur	Terrorist
Characteristic	Planning	None	Possible	Definite	Extensive
	Access	Stealth	Stealth	Stealth	Stealth or overt
	Weapons	None	Knife or pistol	Explosives	Any
	Contaminants	None	None	Possible	Probable
	Asset damage	Minimal	Minimal	Significant	Extensive
	Theft	None	Probable	Possible	Possible
	Injuries	None	Possible	Possible	Extensive
	Fatalities	None	Possible	Possible	Likely

1.5.1.2 Secondary Benefits of Designing for Security Against Malevolent Events

Utilities that have incorporated security for malevolent events are also finding that they have enhanced their response to natural disasters and unanticipated failures and can restore system operation and service more quickly. Water utilities have traditionally done an excellent job in developing strategies for responding to natural events and unexpected system failures. Natural events can include acute events such as violent weather, earthquake, fire, or flood, as well as chronic events such as drought or expansive soils.

Because natural disasters tend to be geographically specific, not all water systems face the same threats. Water utilities typically have countermeasures in place to mitigate the threats from natural disasters common to the geographic area because building codes and standard engineering practices consider natural threats in design standards and regulations (e.g., structures designed to withstand 120 miles per hour winds in hurricane prone areas). In addition, water utilities usually have disaster preparedness plans and, possibly, response and recovery plans as well.

Unanticipated failures that can have a great impact on a water utility can include hazardous material release, power or telephone service disruption, infrastructure failure, or even a labor strike or slowdown. Standard operating procedures, key contact lists, and a complete inventory of emergency parts and supplies are ways in which water utilities can respond to these types of crises.

1.5.1.3 Management, Operations, and Security Design Enhancements to Mitigate Malevolent Acts

The plans, processes, and procedures used to mitigate malevolent acts, as well as natural events and unanticipated failures, are many. Some of the typical security enhancements for water systems that mitigate these events include the following:

- Redundant systems
- Operational flexibility in design

- Operational backups
- Backup power systems
- Alternate connectivity to other water supplies
- Uninterruptible power supply (UPS)/power filtration
- Increased treated water reserves
- Reduced quantities of hazardous materials (e.g., chlorine gas)
- Modified treatment process that is less hazardous
- Improved building design, construction, and materials
- Multiple sources
- Distributed treatment

1.5.2 Generic Threat Levels

The Department of Homeland Security has developed an advisory system that identifies the present threat to the United States. In addition, the Water Information Sharing and Analysis Center (WaterISAC) advisory system (sponsored and developed by the EPA and AWWA) is another means that can be used to communicate rapidly with water utilities about threats and threat levels. Utilities need to be knowledgeable about how their operations and operational procedures should be adjusted to coincide with these generic threat levels. Understanding the utility-level actions at the different Homeland Security Advisory System levels (sample actions are shown in Table 1-3), reviewing relevant materials, and planning are important for proper control and response actions. In support of a utility’s ERP, the EPA also provides guidelines for response in its Emergency Response Protocol Toolbox (USEPA 2003). A summary of a portion of that guidance, provided in Table 1-4, demonstrate good first steps.

TABLE 1-3
 Actions Based on Threat Level as Announced by the Department of Homeland Security (DHS 2004, EPA 2004a)

Threat Level Announced	Local Actions to Perform
Low (Green)	Normal operations. Focus on facility assessments and ERPs. Review plans for contingencies, and make sure checklists and other information are current.
Guarded (Blue)	Normal operations. Advise employees of the status change; prepare to communicate with first responders and other agencies; review ERPs.
Elevated (Yellow)	Advise all employees of the status change. Have employees intercept and report all visitors. Follow all utility-specific guidance for restricted access.
High (Orange)	Double the frequency of checks on remote system operations. Review and re-stock emergency use supplies as required. Fuel all vehicles, generators and equipment. Charge all batteries.
Severe (Red)	Cancel visits. Prepare for extended-hour work shifts. Stockpile reserves, such as fuel. Maximize water storage.

TABLE 1-4

Summary of EPA Water Utility Response, Recovery and Remediation Guidance for Man-made and/or Technological Emergencies

I. Contamination Threat to the Water System, Unknown Contaminant, Unknown Location		
Source Water	Treatment Facility	Storage/Distribution
Notify local law enforcement, local Federal Bureau of Investigation (FBI) field office	Notify local/state emergency management organizations, notify ISAC	Notify other associated system authorities
Increase sampling at or near system intakes	Preserve latest full battery background test as baseline	Review ability to isolate storage and distribution zones
Review ability to isolate water source(s)	Increase sampling efforts	
	Review ability to stop treatment and notify customers	
	Coordinate alternative water supplies	
II. Contamination Threat or Occurrence at a Major Event, Stadium, Convention Center, Etc.		
Source Water	Treatment Facility	Storage/Distribution
Notify local law enforcement, Local FBI Field office, National Response Center, WaterISAC	Notify local/state emergency management organizations, notify wastewater system, notify Governor	Notify local government officials
		Coordinate system isolation plan
		Assist in draining contained water
		Assist in developing sampling plan
		Provide alternative water sources
III. Notification from Health Officials of Potential Water Contamination, Public Cases Identified		
Source Water	Treatment Facility	Storage/Distribution
Request information on symptoms, potential contaminants and potential area affected	Notify local law enforcement, local/state emergency management organizations, FBI Field Office, and National Response Center	Notify other associated system authorities, local government official, and the Governor
Increase sampling at or near system intakes	Preserve latest full battery background test as baseline	Increase sampling in the area potentially affected
Consider whether to isolate source water supplies	Increase sampling efforts	Increase sampling at locations where contaminant might have migrated
	Consider stopping normal operations and notifying customers	Consider whether to isolate
	Coordinate alternative water supply if needed	Consider whether to increase residual disinfection levels
IV. Electronic Intrusion of the SCADA System		
Source Water	Treatment Facility	Storage/Distribution
Notify local law enforcement and local FBI Field Office	Notify the National Infrastructure Protection Center	Notify other associated system authorities, and employees
Increase sampling at or near system intakes	Preserve latest full battery background test as a baseline	Monitor unmanned components of the storage and distribution system
Consider whether to isolate the source water	Increase sampling efforts	Consider whether to isolate portions of the system
	Temporarily shut down SCADA and use manual operation procedures	
	Consider whether to shut down system and provide alternate water	

1.5.3 Threat Level Assessment

Identifying the threat level that faces a utility is a critical step in understanding the level of protection required for its water system. The determination of a threat level is composed of two main components:

- First, the type of threat
 - Inside threats (employees, vendors, onsite contractors)
 - Outside threats (vandals, criminals, cyber terrorists, domestic terrorists, foreign terrorists)
- Second, an assessment of the likelihood of a threat occurring at this utility
 - Capability of the threat (e.g., number of adversaries)
 - History of threats
 - Tactics and methods of attacks (including tools)
 - Access to critical equipment (internal)
 - Motivation of adversary

The threat level assessment process includes open dialogue with local law enforcement agencies. This dialogue should include at a minimum conversations with the local Federal Bureau of Investigation, the Sheriff, police department, and undercover task force personnel. Documented occurrences at the utility, using the expertise and experience of the utility's employees, should be reviewed. It is also worthwhile to talk to neighboring utilities regarding past experiences that they have encountered.

Capabilities. The capability of the threats identified is related to the likelihood that an event will occur. Identification of a possible threat, such as a criminal or a terrorist, helps to identify the capability of those individuals to be successful in causing disruptions. The more organized and less spurious the intruder is, the more likely those adversaries will use more advanced equipment and weapons. On the other hand, adversaries may be less likely to approach a facility where they could be easily detected and stopped.

History. Research and discussion with local law enforcement is imperative. Awareness of national or international level security alerts does little to provide a picture of what is happening in local neighborhoods. Regular discussions and information-sharing with the local police, sheriff, and FBI field offices can provide a much clearer potential for man-made activity against utilities. The presence of local extremist groups and vocal activist groups can have a direct effect on calculating the likelihood that an event will occur on utility property.

Utilities should frequently share their events, trespasses, and cyber intrusion cases with their local law enforcement agencies. Sharing knowledge of activities and actions against different parts of the nation's infrastructure aids the FBI, sheriff, and police to better disseminate and evaluate information in each region of the country.

Tactics and Methods. Tactics of carrying out malevolent acts include overt actions and surreptitious actions. Overt actions include direct attack on infrastructure, assault, and hostage taking. Surreptitious actions include vandalism, theft, contamination, use of explosives, and cyber attacks.

Methods include unarmed individuals attacking individuals, damaging equipment, and shutting valves, and using sewers as access-ways to otherwise secure sites unrelated to the utility. Other methods include weapons such as knives, pistols, rifles, or submachine guns, and standoff weapons such as rocket-propelled grenades and mortars. Explosives may be manufactured (e.g., hand grenades) or improvised explosive devices (IEDs) that are placed at a location such as a pipe bomb in a trashcan. TNT, C4, or other high explosive hidden in a vehicle that is parked or driven onto a site and either manually or remotely detonated could be used. Adversaries may also use mail bombs or bombs placed in packages or containers carrying materials that are delivered to the utility.

Contamination with chemical, biological, or radiological agents is a threat from two perspectives. First, these agents may be used against utility personnel through dispersal in the air; through heating, ventilation, and air conditioning (HVAC) systems; food; and the potable water supply. Second, these agents can be introduced to the public through the source water system, directly into the treatment system, or into the water distribution system. Depending upon the specific substances used, damage may be acute and/or chronic.

Water systems also face malevolent acts to their information systems through cyber attacks. Such attacks may originate internally or externally. Attacks directly on the utility may disable a SCADA system and alarms, override process controls, or take over control of key points in the system resulting in water outages or insufficiently treated water. Cyber attacks may also interrupt communications, as well as intranet and Internet services.

Attacks on outside providers, such as power generators or power grid operators, can also significantly affect the ability of water utilities to provide continuous and effective service.

Access. The VA process helps identify those parts of the water system that are critical to maintaining operations. Protection of those key assets, without which the system would not be able to meet its mission, is logical. Providing worker access to those critical assets is important, as is denying access to others. If access to key locations can be achieved without detection and damage done or equipment taken off line, key single points of failure can occur that affect other related and unrelated parts of the process.

Motivation. The motivation of perpetrators ranges from the mischief of vandals to the desire of adversaries to undermine the well-being of society. In between these two extremes are a variety of motivating factors that include persons angry at the utility or individual of the utility. Disgruntled employees who feel abused, belittled, unappreciated, or unrewarded may attack coworkers or supervisors, damage infrastructure, destroy or change data, or steal equipment. Former employees who believe they were wrongly terminated or desire to avenge a previous incident may return to the workplace and commit an assault or murder, property damage, theft, or sabotage. Spouses and partners of disgruntled employees and former employees may commit the same acts of revenge on the utility or its management. Similarly, customers who believe they were wrongly treated, overcharged, or who have experienced property damage may vent their anger in similar ways. It is important to realize that the actions taken by these angry persons may be either planned or impulsive.

Economic gain may motivate persons, including employees, to steal equipment, supplies, vehicles, or money. Such thefts may be a single breaking and entering, making the crime obvious. On the other hand, thefts may be insidious if committed by persons such as employees, vendors or contractors who have access to the organization's facilities. Theft may also be conducted through an ongoing scheme that involves stealing of rarely used items or embezzling small amounts of money, and covered up through unauthorized adjustments to inventory or financial records. Such crimes may remain unnoticed for long periods of time. Theft by employees are unfortunately common. It is estimated 68.6 percent of employees who commit these crimes have no previous criminal record.¹

At the extreme end of the motivation scale are the driving forces of the terrorist. While remaining a topic of debate, motivating factors may be political, religious, social, or symbolic; revenge, change, or the desire to gain attention may instigate it. There are two categories of terrorists: international and domestic. International terrorists act with the intent of undermining stability and instilling terror through destruction of economically important and symbolic assets, and, potentially, by killing large numbers of people. These terrorists almost always work in groups, and spend considerable time and resources to select and learn about their targets, and plan their attacks. At the extreme end, the motivation of terrorists is so strong that they will adopt different lifestyles, deceive and betray friends and family, and sacrifice themselves for their cause. Domestic terrorists may have a well-financed, loose-knit working organization focused around their cause, but usually work alone.

1.5.3.1 Locate Information on Most Probable Threats

There are a number of sources that utilities can use to obtain local information on most probable threats. As discussed in Section 1.5.2, "Generic Threat Levels," Water ISAC, operated by the Association of Metropolitan Water Agencies (AMWA), can be consulted for current information on security intelligence in the water industry. Additionally, information to supplement the utility's knowledge and experience can be obtained through communication with law enforcement and other utilities.

1.5.3.2 Use the Information to Review the Utility's Organizational Security Strategies

Utilities can use a variety of existing information as part of reviewing their current organizational security strategies. Some of the typical information that is readily accessible to utilities includes the following:

- Operations and operational capabilities
- Current policies and procedures
- General physical security capability
- Maintenance and testing of security systems

¹ *Detecting Employees Who Steal*, Workforce Management, November 2002, page 31

1.5.3.3 Identify Response Capability and Actions

Response capability refers to a range of actions from appropriate water system operator responses to police responses to the involvement of other public safety agencies. It also includes the built-in operations responses within the water treatment and delivery system itself. It involves the assessment of what is wrong and the decision of what to do about it. Response is based on the threat identified in relation to the critical asset that is threatened.

1.6 Developing a Security Strategy

A security strategy is both a short-range list of activities and a long-range plan. Security strategy is not developed as a stand-alone exercise, but requires an understanding of the information previously introduced in this section.

Understanding system vulnerabilities, or critical “points of failure,” that would keep a utility from achieving its defined mission goals is the first part of a necessary strategy. How to keep in business is the focus of the strategy. Any action to improve system redundancy, protect critical functions, back up operations, train personnel, and organize business policies, procedures, plans, and functions supports the goal of continuing the mission without interruption.

There are multiple parts to a good security strategy. Defining a goal of complete system redundancy – of pumps, tanks, water sources, and other essential facilities – would be a long-range plan. Addressing immediate issues identified in a security plan can help to reduce risk quickly by focusing on management and operations activities under current control. When utilities perform this analysis, it is important that they consider not only documenting the process, but also communicating the assumed risk tolerance to policy makers and governing boards. It is critical for utilities to have policy makers aware of and in agreement with utility management with respect to the degree of risk tolerance selected. The level of acceptable risk tolerance that utilities can agree to is subjective and can have considerable impact on the cost and degree to which utilities undertake security improvements, change operating policies and procedures, and so on.

This guidance provides a broad range of tools and techniques to address water system security. Some are simple and easy to implement; others are more complex and costly, possibly requiring a significant involvement of time and resources. It is essential for utilities to realize that an effective security plan is not necessarily complex or expensive. An effective security plan is one that makes sense for and can be implemented within existing (and future) conditions. Utilities are encouraged to apply the contents of this guidance in a commonsense and practical way.

The following sections can help with the development of a good security strategy.

1.6.1 Determining the Required Level of Security

As described in Section 1.2, a vulnerability assessment typically uses a risk-based approach to prioritize potential security improvements. A vulnerability assessment does not, however, determine the levels of risk, and thus security systems, that are acceptable and how the potential improvements should be implemented. Many vulnerability assessments include determining the DBT, which

identifies the types of adversaries and their capabilities; however, the assessments generally provide limited guidance regarding how to select the threat. Methods that can be used to determine the level of security improvements that should be implemented are described below.

1.6.2 Conducting a Risk Reduction Analysis

Risk is best assessed and analyzed if quantified (e.g., 1 to 100). Because risk is related to the likelihood of occurrence (probability) and the severity (criticality) of the consequence. To generate a quantified result, both probability and criticality should be stated in the same scale. Risk reduction is then accomplished by reducing either the likelihood of occurrence, the severity of the consequence, or both. The approach should be to optimize risk reduction, that is, to reduce as much of the risk at the least cost through a cost risk-reduction analysis that leads to prioritizing countermeasures.

1.6.3 Conducting a Cost-Benefit Analysis

A cost-benefit analysis can be performed for security improvements as is commonly done for other engineering alternative evaluations. A cost-benefit evaluation is most robust if benefits can be readily quantified. For example, the cost of improvements in physical security (such as improved locks, alarms, and fencing) can be compared to the value of avoided vandalism damages. Establish baseline information by collecting information on historical events, such as:

- “tagging” events, trespass events, and unescorted visitors
- frequency and cost of fence and gate repairs
- system breakdowns (e.g., pumps, valves, filters, etc.) and the duration of out-of-service events
- supply equipment lead times
- personnel overtime events due to system problems

When considering design changes to operations, procedures, or physical security, a continued review of the baseline indicators can provide documentable comparisons to the cost of doing business before and after implementing changes.

1.6.4 Conducting a Cost-to-Risk-Reduction Analysis

Security improvements can also be prioritized by comparing the cost to implement each security measure against the degree of risk reduction that the measure would provide. For risk assessment methodologies such as RAM-W™, the amount of risk reduction can be expressed numerically by determining the risk score for each asset before and after the proposed security improvement. This analysis typically shows that measures requiring a relatively low capital investment, such as implementing security policies and procedures, result in a low cost-to-risk reduction ratio. As shown in Figure 1-5, a cost-to-risk-reduction curve can be generated, and a determination can be made as to what measures should be implemented by identifying the “knee of the curve,” or the point at which the risk reduction associated with implementing additional costly security measures is marginal.

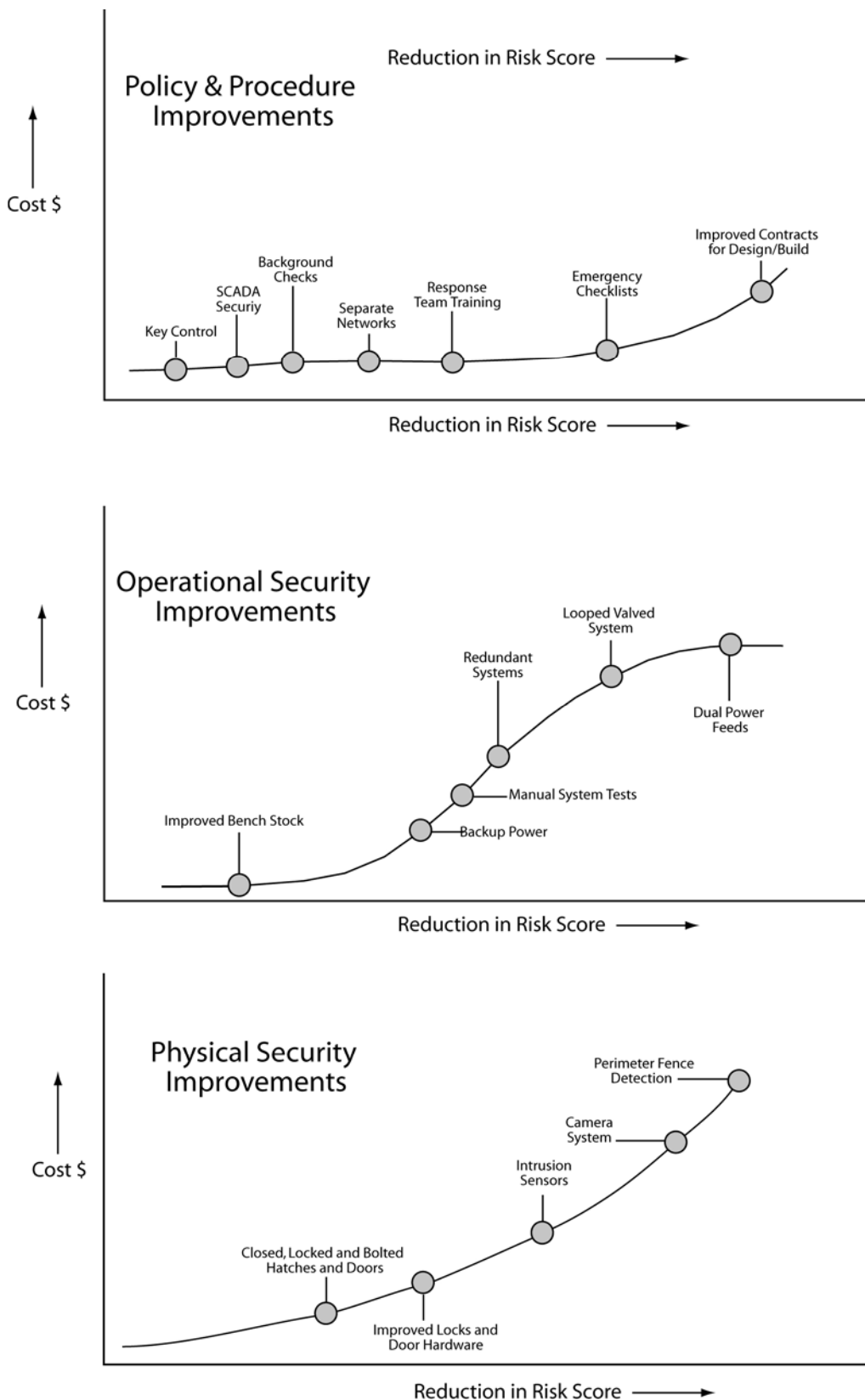


FIGURE 1-5
Sample Cost to Risk Reduction Curves

1.6.5 Comparing Security Risks to Other Risks

Utilities face many risks other than those from malevolent acts that could substantially disrupt their ability to meet their mission. Another prioritization method that can be used is to compare security risks to these other “non-security” risks using a common ranking scale. Failures of major facilities or pipelines due to obsolescence, water quality violations, and unexpected losses of key staff are examples of risks that utilities must actively manage.

A utility can put its security risks in context by conducting an overall operational risk analysis in parallel with the vulnerability assessment. While one type of risk is usually not compared to an operational facet, both can affect the mission of the utility. Risks and issues that affect the ability to disrupt the mission can be ranked one above or below another. Although the consequences of a malevolent act could be high, the probability of occurrence may be relatively low.²

1.6.6 Developing a Balanced Plan

The concept of balanced approach to security involves more than physical additions like fences, guards, and dogs. These design approaches to improved security can be grouped into two general categories – Basic and Advanced. Basic changes are those that can be implemented more quickly or with fewer changes, and can occur across the organization in terms of Procedures, Operations and Physical Security improvements. Examples of such changes include:

- The design of new facilities and retrofits of existing water system facilities that build in security features. The training of personnel to observe, control, and respond to deliberate actions against the utility. Without staff commitment to the security program, which will require a cultural change in the way that business is conducted, the program will not be effective.
- Procedures and checklists that allow for recognition of problems and specify proper reactions to problems.
- Systems that are operated and maintained for depth of capability and ease of control, including methods to assess an alarm situation through the use of intrusion sensors, cameras, and other technologies. Detection of deliberate actions against a water system can be determined in a variety of ways. On-line monitors and system parameter guidelines indicate when a parameter is out-of-bounds. Placing monitors so that they can quickly pin-point aberrations in operational parameters provides real-time capability to mitigate intrusions.
- The proper response to mitigate activities designed to keep a utility from meeting its mission objectives.
- The steps necessary to return to normal operations quickly, efficiently and in a manner that allows everyone to learn and improve so as to avoid a future occurrence with the same impact to operations.

² It is challenging to quantify the probability of a high-level adversary attack given the absence of incident history, while it is relatively easier to estimate the probability of low-level threats like vandalism given that there is more likely to be an incident history from which to draw.

These approaches can be organized into four categories—prevention, mitigation, response, and recovery—with examples provided below. Detailed information can be found in subsequent sections.

1.6.6.1 Prevention

Proactive work by utilities on prevention can reap substantial benefits by securing their water systems from malevolent attacks. Some examples of preventative measures for considerations follow.

1.6.6.1.1 Basic

Consider contracting with a computer security consultant to conduct a periodic audit of the firewall, routers, and intrusion system. A consultant can relieve the burden of maintaining a high level of expertise in this area. Balance the need to establish monitoring programs with the need for discretion regarding water utility critical assets.

1.6.6.1.2 Advanced

- Continuously coordinate vulnerability assessment activities with other nearby utilities, including organizations that control the source water used by the utility, and participate, to the extent possible, in assessments conducted to determine that critical water sources and critical operations are appropriately monitored and adequately protected.
- Work with chemical suppliers to initiate use of anti-hijacking technologies and to develop utility-supplier protocols for preventing and responding to tampering during shipment.
- Establish a citizen's watch program and a law enforcement education program to help provide monitoring of hydrants and water utility system sites with the intent of preventing unauthorized use or entry.

As part of a long-range plan, some utilities may choose to upgrade the current backflow prevention system by installing backflow prevention devices on commercial and industrial customers that pose high risk to the water system. Utilities may also choose to eventually install backflow prevention devices, such as dual check valves, on residential homes as part of a planned meter replacement program that is part of their long-range Capital Improvement Programs.

1.6.6.2 Mitigation

The ability to prevent a deliberate and planned attack is always limited. The ability to control the events offers a chance to mitigate the effects of a malevolent event. If water is contaminated or shut off and the system has means to deliver potable water in other ways, then the effects of the attack have been mitigated. Redundant delivery systems, backup power, and alternate treatment options, for example, can mitigate a variety of man-made or natural disasters. To effectively mitigate, a utility first identifies the parts of the operation that present the most risk or cannot be easily mitigated, then conducts a risk reduction analysis. Risks and subsequent mitigations are identified and prioritized until all have been considered.

Some malevolent events will be outside of the utility's control or just not practical to prevent from occurring. Below are some ways that utilities can mitigate these types of events.

Basic

- If a utility uses groundwater, reconsider developing a wellhead protection program to provide additional protection to the aquifer.
- To lower consequences of critical asset damage, standardize equipment and maintain spare parts or identify contractors that can supply these parts on short notice.
- Back up computer system data routinely.
- Identify secondary location for the operating control room.

Advanced

- Develop a computerized water quality/hydraulic monitoring system of the distribution system that is linked to an integrated geographic information system (GIS) database for critical facilities.
- Consider installing real-time monitoring equipment that has recently been developed to enable the direct detection of chemical contaminants in water distribution systems.
- Improve the electrical power feeds to the facilities. Redundant electrical power systems significantly reduce the vulnerability risk to essential operations. Options for providing redundant systems include installing sufficient backup generator capacity to operate the majority of the treatment processes or installing an electrical feed from another power provider.

1.6.6.3 Response

Utilities cannot initiate a response to an event until detection and assessment of an intruder alarm or the actual intrusion has occurred. Initiating response will typically require the notification and cooperation, and will benefit from a good working relationship with, law enforcement. Additionally, EPA's Response Protocol Toolbox is a good source of planning information. Below are some suggested tools that can be adopted by utilities to improve detection, assessment, and response to malevolent events.

Basic

- Develop procedures to respond to a security breach located at any water treatment plant (WTP) facility (including alarm systems). Coordinate with local law enforcement.
- Identify high-priority facilities and work with local law enforcement to improve response time to these critical facilities.
- Institute a policy that operators and maintenance workers contact the SCADA/alarm monitoring stations when site buildings and alarmed doors are accessed for operational purposes.

Advanced

- Purchase a "panic button" system to be worn by the operators and maintenance staff that enables the staff to send a distress signal to the local law enforcement agency in an emergency situation.

1.6.6.4 Recovery

Recovery is a critical part of a utility's balanced approach to securing its water system against malevolent events. This part of the approach refers to the ability of the utility system to return to full

operation. The best outcome of a deliberate malevolent act is for the public to be unaware of the event – that the systems, plans, and responses are able to restore services within the reserve capacity of the system.

The goal of the recovery phase is to return the system to its optimal operational status as soon as possible. Follow-up actions are also needed to learn and improve; document costs in resources, time and labor; and to provide information to other agencies that can help to improve identification, tracking, and prevention of future events.

1.6.7 Prioritizing Security Investments

Typically, developing a vulnerability assessment involves defining a relatively long list of vulnerabilities and potential improvements, ranked according to the potential risk. When presented with this list, utilities are able to contemplate how many of the recommendations to implement and the level of protection that is acceptable. In prioritizing security investments, they need to consider limited resources and balance the external demand for security with the internal resources available to implement security measures. In addition to the legal considerations described earlier, there are other considerations that may be addressed in answering this question.

1.6.8 Documenting the Process

Utilities need to thoroughly document the risk reduction analysis and mitigation decision process and keep the documentation in a secure location with restricted access. The document is the utility's roadmap to protecting its system.

1.6.9 Sharing Information

Utilities have a number of opportunities to share information that can reduce costs of enhancing physical security of their water systems.

- Benchmarking and other industry activities. Participation in benchmarking or other related industry activities can provide the utility with early access to best management practices that can be cost-effectively integrated into the program.
- Provide cyber attack details to the local FBI office. The local FBI has established capabilities of researching and investigating both successful and unsuccessful cyber attacks on utility systems.
- Coordinate/cooperate with contiguous utility systems. Coordination of security-related programs with contiguous systems can provide additional redundancy and potentially reduce the costs of securing the utility's water system.

