ABSTRACT

The security of the Province’s water and wastewater infrastructure has always been important but in recent years has taken on a new priority. Few public utilities have the immediate, direct and long-term effect on public health, safety and consciousness, as community water infrastructure does. This paper and discussion will address both the issue of accomplishing effective infrastructure security assessment and protection in the post-9/11 context during challenging economic times and the need for an all-risk approach that would cover natural and operational hazards. A description of asset identification and criticality rating, threat and vulnerability assessment procedures, and gap analysis and security master planning methodologies is presented. The Risk Assessment Methodology for Water (RAM-WSM) developed by Sandia Corporation, and which now constitutes the standard security risk assessment tool for water utilities, is summarized.

INTRODUCTION

The September 11, 2001 attacks on the Pentagon and World Trade Center towers have drawn significant attention to the security of public and private institutions and systems in Canada, including the water infrastructure facilities and assets of British Columbia. The Province’s water supply and water quality infrastructure have been recognized as being potentially vulnerable to terrorist attacks of different types, including physical disruption, structural damage, bio-chemical contamination and computer systems cyber attacks. In general, damage or disruption to the Province’s water supply and water quality infrastructure by natural (earthquake, storms, flooding, etc.) or man-made threats (terrorism, sabotage, human error) would cause disruption to the delivery of a vital service in the Province, eventually threatening public health and the environment, and possibly causing loss of life.

Although not considered to be immediately subject, public utilities are, by their very nature, vulnerable to mischief, vandalism, sabotage and terrorism. Recent world events have attracted the attention of domestic extremists and international terrorists to the relatively weak security profiles of most critical public infrastructure facilities. The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) issued a series of releases during 2002 reporting that terrorist organizations, notably Al Qa’ida, have shown heightened interest in water supply and SCADA systems. US intelligence and law enforcement agencies have received indications that international terrorist organizations have sought information on SCADA systems and pursued details of water and wastewater management practices in the United States. The Canadian Security Intelligence Service (CSIS) has been cautious in its description of the terrorist threat in Canada but has publicly recognized that our close cultural and economic ties with the US as well as our participation in the War Against Terrorism in Afghanistan could see Canada or Canadians targeted for attack. In the past, Canadians could have been forgiven for believing that terrorism was something that happened to other people far away. While some Canadians have been victims of terrorist attacks - most notably in the 1985 bombing of an Air India flight from Toronto, Canada, as a country, has not often been specifically targeted for attack. However, at 8:46 a.m. (Eastern Standard Time) on September 11, 2001, when the first of two aircraft crashed into the World Trade Center in New York, the rules changed fundamentally and, maybe, irrevocably.
Not only were there a number of Canadians among the approximately 3,000 victims of the attack but, because of Canada’s solidarity with the United States in pursuing those responsible, our country - along with other western democracies - has now become a potential target for terrorist activity.

The threat from terrorism is real, it is immediate, and it is evolving. State sponsored terrorism appears to have declined over the past five years, but transnational groups— with decentralized leadership that makes them harder to identify and disrupt—are emerging. We are seeing fewer centrally controlled operations, and more acts initiated and executed at lower levels. Terrorists are also becoming more operationally adept and more technically sophisticated in order to defeat counter-terrorism measures. For example, as we have increased security around government and military facilities, terrorists are seeking out "softer" targets that provide opportunities for mass casualties. Some groups are acquiring rudimentary cyber-attack tools. Terrorist groups are actively searching the Internet to acquire information and capabilities for chemical, biological, radiological, and even nuclear attacks. Many of the 29 officially designated terrorist organizations have an interest in unconventional weapons, and Usama bin Ladin in 1998 even declared their acquisition a "religious duty."

The Royal Canadian Mounted Police (RCMP) Criminal Intelligence Directorate published a secret report in October of 2002 that stated in part “Any US military action in Iraq will likely be interpreted as an unprovoked act of aggression that many Islamic extremists will use to initiate further terrorist activities against US targets and their allies around the world.” The threat of international terrorism is aimed primarily at the governments of Israel, the United States, Great Britain, and most recently Australia. While Canada is not immune, it does enjoy a relatively low incidence of violent acts of terrorism. However as Canada becomes more integrated with these countries, it will be seen by extremists and terrorists to lose its most distinguishing characteristic, that of being a separate and sovereign nation. The potential consequence is an increase within our borders of both domestic extremism and international terrorism. And, the trend towards greater lethality will continue. Between now and 2015, terrorist tactics will become increasingly sophisticated and designed to achieve mass destruction and casualties.

The Criminal Intelligence Service Canada (CISC) 2002 annual report emphasized the need for increased awareness of organized crime’s link to cyber-crime and its potential affect on business. Organized crime groups are well known for their use of sophisticated technology to commit crimes and have increasingly adapted to the use of cyber-space with its added benefits of global reach and anonymity. One of the most recent and troubling dynamics with respect to criminal enterprise is the potential for the development of strategic and operational links between organized crime, domestic extremist and international terrorist groups. To make matters even more challenging, the dark side of information technology’s evolution continues to open uncharted territory for criminal and terrorist exploitation. While in some cases these crimes are new, in other instances they are not. In many respects, information technology has simply facilitated the commission of old crime types in new ways.

BACKGROUND

Properly carried out, vulnerability assessments of water infrastructure and systems help evaluate susceptibility to potential threats and identify viable corrective actions that mitigate the risk of serious consequences from man-made threats (e.g. vandalism, insider sabotage, terrorist attack, etc.). Such an assessment for a water system would take into account the vulnerability of the water supply (ground and surface water), its treatment and distribution systems. Risks posed to the water system of the community served, related to attack, natural and operational hazards can be quantified. A proper hazards evaluation would serve as a guide to the water utility by providing a ranked plan for security and physical upgrades, modifications of operational procedures, and the necessary policy changes to mitigate the risks, vulnerabilities and security gaps to the infrastructure’s critical assets. A well-conducted water infrastructure vulnerability assessment provides a comprehensive framework for developing risk reduction options and associated costs.
The way in which the vulnerability assessment is performed, as part of a risk assessment methodology, is to be determined by each water utility. Formal procedural standardization is not established in British Columbia. But it must be remembered throughout the assessment process that the ultimate goal is twofold: To safeguard public health and safety, and to reduce the potential for disruption of both a reliable supply of pressurized water and safe wastewater management.

The following are common elements of vulnerability assessments. They include external natural and man-made risks, and operational hazards (in which some are man-made). These elements are conceptual in nature and do not intend to serve as a detailed methodology:

1. Characterization of the water infrastructure system, including its mission and objectives;
2. Identification and prioritization of all external events, natural and man-made, and operational adverse consequences to avoid;
3. Determination of critical assets that may be subject to natural events and malevolent acts and operational risks;
4. Assessment of the likelihood (qualitative probability) of such events and acts from adversaries;
5. Evaluation of feasible countermeasures (risk mitigation) and their cost for implementation;

The vulnerability assessment process will range in complexity based on the location (local seismicity, geotechnical hazards, physical exposure) and the design and operation of the water system itself. The nature and extent of the vulnerability assessment will differ among systems based on a number of factors, including system size, potential population affected, source water, treatment complexity, system infrastructure and other factors. Security and safety evaluations, in themselves vary, based on knowledge and types of threats, available security technologies, and applicable local, provincial and federal regulations.

Water and wastewater infrastructure is normally comprised of many complex components. It is paramount to improve the performance of the entire system rather than optimizing the performance of the individual components. These components must work as an integrated whole otherwise the security and risks mitigation objective will not be achieved. This way, the ability to assess critical interactions would help determine where failures and security gaps occur. In the case of assessing the security risks, the first component to be investigated is the sources or supplies of water. Here we include rivers and streams, lakes, water wells and reservoirs.

The case of contamination of large volumes is likely to require overcoming the typical significant dilution to pose a life-threatening dose to the end user. Obviously, as the water volume decreases together with the potential for dilution, the risk of effective contamination increases. This is the case of drinking water intakes on rivers, where each of these intakes can be vulnerable to accidental or intentional release of toxic chemicals or biological substances. Contaminating agents can then be deactivated by filtration or by treatment common to water treatment plants. The risk of contamination is mitigated via early warning systems, where real-time monitoring systems and sensors are required. These real-time monitoring devices can be used throughout the water infrastructure system. To be effective, they should have certain characteristics such as being integrated with multiple sensors, cover most if not all potential threats of contamination, remote sensing capacity, blanket installation of monitoring devices, continuous functioning and simple results interpretation.

For most water utilities, the water treatment facility is next normally assessed for security risks. The chemicals employed would normally have limits in their injection rates through remote control using Supervisory Control and Data Acquisition (SCADA) computer systems. These systems are a concern due to the threat of cyber attacks. Computer control systems will control operations and monitor system status. With automation being implemented over the past few years, they end up being practically stand-alone systems vulnerable to hacking.
After treatment, the water either enters the distribution system or is being stored. The distribution system can be easily contaminated. Human error or accidental backflow can cause contamination. Accidental or intentional contamination is still a rare occurrence, but a potential vulnerability. Monitoring capabilities are needed in the distribution system.

Should the water supply, water treatment facilities or distribution systems be disrupted and rendered inoperable, in time the wastewater system will be inoperable. Collected wastewater is sent to the wastewater treatment plant. This wastewater component is integral part of the total system. If this water is prevented from being treated, not only there can be a health concern in populated areas, but also significant impact on downriver water intakes. The outfall of wastewater treatment plants sometimes end up being major tributaries of some rivers and can become a significant part of the water supply for the next intake downstream.

Water infrastructure is interdependent with other infrastructure. Electric power supply is required along distribution lifelines and back-up power supply is recommended. Counter-measures against disruption along lifelines are still not installed in many large water utility systems throughout North America. Likewise, the transportation system (rail and highway) and chemical industry supply chains should not be interrupted. These components can also be regarded as lifelines, similar to water distribution networks, and prompt restoration of services and emergency planning in place are necessary when disrupted.

ENTERPRISE SECURITY AND RISK MANAGEMENT PLANNING

A Security Master Plan is a comprehensive multi-year document business plan that articulates the threat-risk assessment, Policy, Procedures, hardware, software, employee training and financial and other data that justifies and supports the investment in a security program. This section is included as a general guideline and preamble to any security Risk Assessment Methodology designed for water and wastewater infrastructure.

Stantec Inc. has developed a Security Master Plan methodology that incorporates five main components for Enterprise Security and Risk Management Planning.

1. Asset Identification and Prioritization
2. Threat Profile
3. Security Profile
4. Gap Analysis
5. Plan Development

These components work collectively answer the main questions of Security Management and Risk Engineering:

What are we protecting?
What are we protecting it from?
How are we protecting it?

Asset Identification

The asset identification process can be performed in several ways. Typically, the users of a facility are the most knowledgeable about it, and can provide the best insight into the operational value of the various assets. Therefore, a detailed questionnaire is a good starting point to determine the relative asset
values. This will provide a subjective view of relative value. To utilize a more quantitative approach, the concept of asset pairing, as used in the Sandia RAM-W system, will ultimately rank the assets on a point scale, and weight them by value. It is important, however, for the professional performing this process to include persons other than the operational personnel in this process. Typically assets are given priority based on their value in helping the organization meet its mission goals. However, the operational and corporate goals both must be met, and in order to meet corporate goals (e.g. – maximize shareholder value) input from senior management in this assessment process is a requirement. Once this process is complete, we will have a picture that details not only what the assets are, but also how they appear in relative importance to each other.

**Threat Profile**

The threat estimation component is again an information gathering exercise. The end result is the development of the Enterprise Threat Profile. Information is gathered from all sources – local, regional, national, and international. While some of this information is available to anyone, often the more sensitive or hard to unearth data is the product of extensive contacts at various levels of government, policing, military, and intelligence agencies. The information garnered will help the aid the risk assessor in determining the critical points regarding any threat.

The questions that the Risk Evaluation component will answer include issues such as

- The existence of a threat. Is there an adversary or adversaries present, or capable of gaining access to the facility?
- Are there outsiders who have a history or known intention to attack this facility or facilities of this nature?
- What was the motivation for these persons or groups in the past?
- What might their present or future motivation be?
- What tactics can be expected, and what resources are available to the attackers?
- Is there a stated, or direct, threat to this facility or industry?
- What threats are out there, and what is the probability of an event occurring?

The threat side of the risk equation boils down in simplest terms to the following flow:

1. **Identify Event**
2. **Identify Adversary**
   - **Existence**: Is adversary present?
   - **Capabilities**: Is adversary resourced?
   - **Intention**: Does adversary have intention or history?
   - **Target**: Has facility been targeted?

Together, the answers to these questions provide the probability of attack.
Security Profile

Having identified the assets, prioritized them, and identified threats to those assets, the next stage in developing the Enterprise Security Master Plan is the evaluation of the existing security infrastructure. This process when completed provides us with the Enterprise Security Profile. It answers the question raised earlier – What are we doing presently to protect our assets? It must be understood that this step provides a snapshot in time of the existing security culture. The process undertakes to evaluate all components of a security program, not merely the obvious ones, such as guard service or electronic elements.

Development of the security profile includes discussion of the electronic components of security, such as access control systems, CCTV and Digital Video Management Systems, and Intrusion and Fire Systems. These elements of the enterprise plan are typically the highest capital cost, and the most obviously visible aspect of the program. However, there is often a mistaken perception that the addition of physical electronic security is a panacea. In fact, there are numerous documented cases where an organization incorporated extensive electronic systems, and because they were not adequately supported with other security elements, they ultimately failed.

The critical issue in this part of the discussion is the understanding of the term “integrated”. Typically security integration describes the paths of communication between the various electronic components of the security program – how well does the access system speak to the CCTV, how well does the intrusion system integrate with these other two systems? However, the real integration occurs when people are brought into the system. How well the facility personnel accept, use, and understand security programs are ultimately the measure of success.

An effective Enterprise Security Master Plan will look beyond the electronic tools, and attempt to provide supplementary means to achieve security goals in cost effective ways. Here are a few important but oft-overlooked security initiatives that serve to better protect corporate assets, mitigate officer/director liability and improve competitiveness.

Personnel Screening

The most important, valuable and vulnerable assets within an enterprise are its employees. Of the variables that contribute to or detract from success in business, none is more critical than the quality of the people. The processes by which recruitment, selection and hiring of employees occur will determine the quality, efficiency, integrity and success of the enterprise. The issue of personnel screening is a sensitive yet important one. Background checks of prospective employees and contractors serve three purposes: to verify the accuracy and completeness of statements made by the candidate, to gather additional relevant information about the candidate that will enable an informed decision regarding their suitability for employment, and to facilitate their proper placement within the organization.

Records (Security) Classification

Nearly everyone understands the importance and potential vulnerability of computer-based information and takes steps to protect those information sources. However, many do not realize how damaging their print records could become if they were to fall into the wrong hands.

Communications and Information Systems Security

The integrity, reliability and availability of an enterprise’s communications and information systems are critical, not only in terms of their ability to perform the mission, but also in terms of the enterprise’s ability to perform that mission without the threat of performance degradation or service interruption. Mission critical assets include both physical and cyber-based systems essential to the day-to-
day operations of a water facility or any other enterprise. From a national economic security perspective, a business enterprise that falls within the health care, telecommunications, energy, banking and finance, transportation, utilities and emergency response sectors may form part of the national critical infrastructure. Historically, critical infrastructures were physically segregated. Because of advances in technology, however, critical infrastructures have progressively converged and have become linked, sometimes interdependent. Advances in technology have also resulted in a high and growing level of automation in the operation of critical infrastructures. The growth of and our increased reliance on critical infrastructures, combined with their complexity, have made them potential targets for physical or cyber-attacks. Additionally, many facilities now find that operational ease requires external access to control systems. It is here that the greatest danger lies – allowing outside access to the interior of the facility.

Emergency Preparedness & Business Resumption

A disaster is any event that disrupts the organization’s ability to function normally due to a loss of infrastructure or resources. Things that ‘can’t happen’ regularly do. Be they natural or man-made, disasters are inevitable. It’s simply a matter of timing and scale. Typically, when things go bad, they do so quickly. There is little time to plan, assemble resources and establish relationships with recovery and support agencies while a disaster is unfolding. The issues confronting the enterprise respecting its ability to respond to and manage the results of a disaster are numerous but can be rendered down to two fundamental priorities: adequate planning and appropriate resource preparation. Within those two priorities lie numerous tasks, each of which require attention in order to ensure that the enterprise is capable of withstanding the consequences of a disaster. The objective in such circumstances is to protect the enterprise’s ability to continue its mission. A poorly managed emergency can become a disaster.

As national critical infrastructures become interdependent, they are exposed to shared risks that might otherwise be non-existent. The list of disaster types, once confined to those of natural origin, has expanded to include an assortment of ‘information age events’ including hazardous material spills, chemical, biological and radiological incidents, sabotage and acts of terrorism, communications intrusion, system hacking, cracking and viral epidemic, labor disputes and public order emergencies to name a few. The shared use of electronic facilities, communications links, professional services and suppliers increases the exposure that the enterprise faces in its efforts to provide guaranteed service delivery. Interdependency means that the enterprise doesn’t have to be the victim to become a victim. The risks that the enterprise’s strategic partners face are also the enterprise’s risks. The risks that the enterprise faces likewise cascade to the enterprise’s customers, clients, and stakeholders.

In addition to the obvious disruptions that would occur during a disaster event, we must consider the personal preparedness and safety levels of enterprise workers and their families. The emotional impact on each of the workers, depending on where they are and what they’re doing at the time of an event will influence both their availability and ability to contribute to the enterprise recovery effort. This cannot be overlooked.

There is a very definite expectation that public utilities will plan and enact measures that adequately address all of its known disaster risks. Failure to do so would likely result in the assignment of liability which, in addition to the direct costs, could jeopardize the ability of the infrastructure to remain in continuous operation, or if disrupted, resume operations hastily.

Gap Analysis

We have now identified and discussed three of the four components of the Enterprise Security Master Plan assessment phase. We have identified and prioritized the assets, we have considered threats to those assets, and we have taken a snapshot of the security profile of the organization. Gap analysis is the element that pulls the entire assessment program together. The gap to be analyzed is that between the threat
profile and the security profile. In almost every case, we would find that the security profile is exceeded to a greater or lesser degree by the threat. That being the case, recommendations must be made to close the gap. These recommendations will address the different aspects of security that can improve the security profile. This may be better security awareness training, development of policy or procedures, or it may involve the addition of security infrastructure. Ultimately, the goal of the recommendations is to ensure that the security profile of the enterprise meets or exceeds the threat profile developed earlier.

It is important to understand that the gap analysis does consider only technical solutions and recommendations, it in fact is a comprehensive evaluation of all factors affecting the Enterprise’s ability to deter, detect, delay and defend against a known threat.

Plan Development and Implementation

Management approvals are critical to the introduction of a Security Master Plan. Management must not only approve but also publicly communicate its desire for the introduction of organizational safety & security. Security is everyone’s business, and that must be seen to begin at the top. Management must identify, assign and delegate authority in order to empower the people named as being responsibility for Plan implementation. Reporting relationships must be clearly stated and enforced if the project is to be successful.

Supporting policies and procedures dealing with all aspects of safety and security need to developed, tested and approved or, if existing, reviewed and tested against the objectives of the Plan, and revised if necessary. An appropriate budget and resource analysis must occur to establish financial projections outlining capital and operating expenditure requirements. Goals and objectives must be set and clearly spelled out within each aspect of the Plan. Standards and technical specifications must be defined in order to attain a reasonable level of accuracy, reliability and availability. Work action plans must be developed together with team members assigned to each task assignment along with timelines and team assignments, naming task team leaders, members and accountability relationships within each task group. The implementation strategy, which is effectively the roadmap for Plan implementation, once approved by senior management can be presented in a variety of formats, (i.e. Microsoft Project). Audit and performance measurement tools are developed and employed from the beginning of the project to ensure that budgets, deliverables and deadlines are consistently met and enable quick and effective problem identification and resolution.

The final result of this effort is an Enterprise Security Master Plan that provides the business case to proceed with a security program to protect the assets and the mission of the organization.

RISK ASSESSMENT METHODOLOGY FOR WATER INFRASTRUCTURE

We will introduce the general principles behind a security risk assessment methodology for water infrastructure (RAM-W) whose major elements are: Planning, threat assessment, facility characterization and consequence assessment, system effectiveness and risk management. This risk assessment methodology was developed at Sandia National Laboratories, Albuquerque, NM, managed and operated for the U.S. Department of Energy by Sandia Corporation, a subsidiary of the Lockheed Martin Corporation. Sandia is the U.S. Department of Energy lead laboratory for physical security research and development. Cooperating agencies were EPA and AWWA among others. The RAM-W security risk assessment methodology was completed by November 2001.

Standard definitions for risk, risk assessment and vulnerability are maintained throughout the process, i.e. risk is considered a measure of the potential damage to or loss of an asset based on the probability of an undesirable occurrence; risk assessment is defined as the process of analyzing threats to and vulnerability of a facility, determining the potential for losses, and identifying cost-effective corrective
measures and residual risk; and *vulnerability* considered an exploitable security weakness or deficiency at a facility. Decisions for security risk mitigation will be based on being able to identify the existing level of protection, how to balance risk throughout the water infrastructure and what can we afford for enhancements.

At the *planning* purpose level, the mission objective can be established as supplying and distributing treated water, safe storage and the treatment process for consumption. Assets are established to be the people and entities served, water facilities and other infrastructure, equipment, and the treatment and distribution processes. Planning requires a pair-wise importance relative weight (1 to 5) comparison between the relative importance of the different elements of *criteria* that comprise the water infrastructure, such as capacity, geographical extent, critical customers served and water quality requirements. For each criteria, such as capacity and all the others, individual components of the water infrastructure are compared and ranked. A *weighted* criteria is then determined as the product of the sum of relative weights scores for criteria of capacity, geographical extent, critical customers and water quality to that resulting of a pair-wise comparison for individual facilities such as treatment plants, pump stations, etc. At the end of the process, a matrix for all criteria vs. each component of the water infrastructure will contain the sum of weighted criteria, and the total for each component. Then the ranking can be established.

For the *threat assessment* part of the methodology, the historical framework for threat definition is determined. This includes defining different threat types (terrorist, criminal, insider saboteur, computer hacker), medium (bomb, forced entry), the different modes of operation and threat capabilities, and the threat level and its likelihood of occurrence in the water facility and distribution infrastructure. The threat assessment will be a judgment, based on available intelligence and information, law enforcement and open source information, of the actual or potential threat to one or more facilities or programs. The essence of the RAM-W process is the Design Basis Threat (DBT). This is the risk assessment process by which the elements of threat are considered, leading directly to the security measures required to confront this threat.

**DBT** includes consideration of the following parameters:

1. Is the threat internal or external?
2. Is it a person acting alone or a group?
3. Is the threat motivated?
4. Is the threat properly resourced to accomplish their mission?
5. Is the threat viable?

When these factors are considered, the *vulnerability assessment* will result in one or more potential threats to the facility that must be defended against. A secondary part of the DBT is the establishing Threat Path; an analysis of the physical path the threat must take to reach the asset. The security design will then be developed based on these threats.

**Example 1:**

A vulnerability assessment determines that the asset is threatened by an organized, highly motivated group of terrorists. Their goal is disruption of the water supply, and death or injury to users of the system. They are well financed and have the arms and other resources to enter the site and achieve their goals. A security design would have to be put to counter this threat.

**Example 2:**

A vulnerability assessment determines that the threat is a former employee who is severely distressed with his departure. He will act alone, and will try to disrupt service in order to make the utility
look bad publicly. He is not well resourced to operate, and will likely attempt to achieve his ends in a somewhat hap hazard manner, such as by breaking into the plant and coloring the water. A security design would be to prevent unauthorized, undetected access from the perimeter, as well as to ensure tight access controls on former employees.

The DBT identifies and describes categories of adversaries, and is important because it influences consequences, the system effectiveness, the likelihood of the attack and the risk. The Risk Equation is defined as \( R = P_A \times (1-P_E) \times C \), where \( P_A \) is the likelihood of the attack, \( P_E \) is the system effectiveness, \( (1-P_E) \) is adversary success and \( C \) describes the consequence of the disruption. The definition of DBT ends up being a management decision made after gathering information, reviewing operational and legal constraints, and determining funds availability.

**Facility characterization** is determined from: in-site information, characterizing the existing protection and evaluating security measures, customizing the fault tree, assessing consequences, and evaluating the existing SCADA system. Includes review of facility and systems diagrams, determining important operational data, knowledge of property borders and adjacent facilities, security and operational policy and procedures in place, existing threat information, unusual occurrence reports, human component (employees, contractors, visitors, shifts), response time of law enforcement, entry controls.

The assets associated with the SCADA system are assets selected from a security perspective. They are utilized in the pair-wise comparison process described above and are ranked by relative risk to focus allocation of remediation resources. These assets include Standard Operating Procedures (SOP), SCADA security policies, network equipment, personnel training, and security monitoring equipment and protection mechanisms. There are a number of interdependencies associated with facility characterization to be considered: transportation, electrical, SCADA and energy systems; and emergency services.

Facility characterization is done for the source water (site of source, interdependences, geographical locations, redundancy and vulnerable pipelines and for treatment facilities (chemicals used, interdependencies, access control, redundancy and spares, and the characteristics of the treatment process). For distribution and storage facilities: their location information, access control information, and vulnerabilities (pipelines, connections, hydrants, vents, ladders, etc.) are all characterized.

The fault tree mentioned above is a graphic representation, highlighting relationships, of the mission objectives of the water infrastructure and the critical assets that support that mission. They are built from an adversary point of view, thus every event on the fault tree is an undesirable event. The security role is to prevent these detrimental events from occurring, preventing the top-most event from occurring first. The fault tree is developed to relate critical assets to the objectives, which they support. The strategy for defeating objectives can be read from the fault tree. This graphical representation can be generic, applying to all water systems and covering common mission objectives, and as such be regarded as a “road map” for the adversary. And a number of fault sub-trees for different processes can be determined: loss of water sources, disabling water treatment, disruption the ability of distributing water, etc. for the description of a specific water system or facility interruption or impairment. The fault tree can be customized or modified by adding or deleting items on the diagram, based on new information, experience of the assessment team, better knowledge of mission, procedures and systems, new undesirable events. A site-specific fault tree includes all important mission objectives and related critical assets for a specific site obtained modifying the generic tree by addition of appropriate branches, and addition and deletion of undesired events.

Examples of a typical treatment plant fault trees are those that establish threat paths for contamination of water before distribution, disabling the pre-treatment and treatment processes, misuse/damage the process control system, loss of critical pump systems, damage/destroy critical lifelines, and loss of key personnel. For a more generic water system, generic fault sub-trees are determined for the
loss of water sources, the disabling of parts of the treatment process, interruption/impairment of the water distribution infrastructure, loss of pressure in the distribution system, interruption or reduction of the ability to store water, loss of critical valve or pump systems, damage pipelines, power outage, misuse of chemicals, loss of critical communications, contaminate water before and during distribution, use of weapons of mass destruction to injure personnel and public, and compromise Utility image and public confidence.

The objective of facility characterizations is to determine the prioritized critical assets as a measure of Consequence \( C \), i.e. consequence values for undesired events due to loss of critical assets. A consequence matrix is developed for the undesired event and qualitative measures of consequence (L, M, H) associated with quantitative measures of economic impact. Documentation to be reviewed to initiate this process includes facility drawings and site plans with supporting documentation, utility maps (electrical, water, wastewater, etc.), service documentation on past problems, chemical impact analyses, financial records of the facility, documentation on water quality standards and historic public confidence levels. Measures of Consequence are defined by the utility itself defining measures of consequences of disruption and associated dollar values. Measures are both the economic loss itself and the anticipated duration of the loss understanding the system-specific storage vs. demand.

The ranking of the critical assets will depend on the severity of losses. Based on each measure of consequence, the consequences of disruption or failure for each critical asset is determined. Ranking is determined in tabular form from a list of critical assets and overall consequence value. Consequences are ranked for undesired events by relative consequence value. Typical measures of consequence are loss of life, number of illnesses, loss of critical customers, economic losses and loss of public confidence.

To determine the system effectiveness \( P_E \), it is necessary to identify and evaluate security and mitigation features in regards to detection, delay and response. It is also necessary to evaluate policies and procedures in place and determine operational effectiveness. The process steps to determine system effectiveness are: identifying the most vulnerable adversary strategy, create an adversary sequence diagram (ASD), derive the most vulnerable adversary scenario for each undesired event and threat type, summarize the identified vulnerabilities and summarize the system effectiveness values \( P_E \). Determining the most vulnerable strategy would normally require team discussion and consensus. The most vulnerable strategy can be summarized in one sentence: who (DBT), what (critical asset) and how (intention). An ASD is constructed for each critical asset included in the strategy, and the worst case path to critical assets is determined.

A Physical Protection System (PPS) will allow the integration of people, procedures and equipment for the protection of assets or facilities against theft, sabotage or other man-made malevolent attack. The System Effectiveness determination process will identify the most vulnerable adversary strategy, create an ASD, derive the most vulnerable adversary scenario for each undesired event and threat type, estimate system effectiveness \( P_E \) for each scenario and identify protection system vulnerabilities. Then the identified vulnerabilities and \( P_E \) values can be summarized. As an example consider the vulnerabilities at a water treatment plant to an outsider threat: Detection: no sensors or assessment capabilities during operational hours, few personnel during off hours; Delay: no barriers; response: Response time not reliable, local police does not have access to locked facility; Mitigation: no spare pumps.

The RAM-W Methodology will identify numerical risk relative values for likelihood of occurrence: \( P_A \) (set normally as 1.0); Consequence \( C \) and \( P_E \) (L=0.1, M=0.5, H=0.9). Upon completing the risk analysis, mitigation objectives can be established (Risk Reduction). The protection objectives are to prevent the undesired event, mitigate the consequences of such event and protect against DBT. The physical protection and operational upgrades are considered to prevent the undesired event though assessment of detection features, delay barriers, time for response and mitigation feasibility.
General practical steps to achieving a feasible risk mitigation strategy should be based in the following general practical steps. a) Develop and implement policies and procedures; b) security training both for the general population as for key personnel at the water facility; c) count with ‘spares’ to be located off-site or very well protected in-site. Spares can be shared between utilities and meet minimum emergency requirements. d) Install back-up systems through alternate energy sources, agreements with local energy providers and mobile systems; e) Establish redundancy, both through multiple paths and through multiple sources.

Electrical pumps and chlorine cylinders are critical assets. For electrical pumps, install natural gas pumps to mitigate the interdependency risk with electrical power. Store spare pumps at another location. The water storage capability can be augmented within the system to allow for outages. The speed at which pumps are replaced must be tested. Other consequence mitigation strategy are increasing the capacity of other treatment facilities, tie-in t neighboring facilities and work with electrical utility to quickly connect to power system is case of intentional disruption. For chlorine deposits, lower the amount on-site, use different disinfectants, store spare tanks off-site and perform training and emergency response exercises.

MITIGATION FOR WATER AND WASTEWATER INFRASTRUCTURE AT RISK

Water infrastructure is vulnerable to four broad classes of terrorist attack: Chemical contamination, biological contamination, physical disruption and disruption of the computerized control network known as the SCADA system. At the same time, security risks are not the only hazards to water infrastructure in British Columbia. Natural and operational risks have to be addressed through implementation of mitigation plans, result of all-risk assessments that consider the full range of possible threats the facilities and infrastructure will be potentially subject to throughout its operational life. Besides, water infrastructure is subject to additional needs and financial requirements:

- Increased monitoring and reporting. Over the last few years, these requirements have augmented significantly;
- New facilities. There is a continuing need for investment in new facilities to keep pace with population growth. These facilities would have to be designed to remain operational after events such as earthquakes or explosive terrorist attacks;
- Aging infrastructure. Older facilities, to remain operational, require a large maintenance and upgrade investment, including that of seismic rehabilitation for structures, floor-mounted or suspended components and lifelines;
- New contaminants. Additional financial investments will be required to address the large number of new contaminants that are soon to be regulated, notwithstanding those contaminants yet to be studied or identified;
- More stringent standards. It is expected that many of the standards for regulated contaminants will become more stringent in the future.

A phased approach is recommended to improve the water infrastructure security in British Columbia. The phases to reduce identified (or to be identified) hazards to the water infrastructure include a short term action plan to be implemented in one to three years and that will basically address security issues and critical (high risk) operational and structural upgrades to the existing infrastructure; an intermediate term plan that can be completed in three to five years from now; and a long term action plan from five to ten years in the future. In all cases, a cost-benefit analysis to assess the risk reduction option vs. the cost of upgrade is to be performed as a decision making tool. This analysis is to be conducted by qualified and experienced risk engineering specialists. It is the water infrastructure management’s responsibility to retain the security and risk management professionals to do this work.
A. Short Term Action Plan

- **Threat Definition.** Perform the security and all-risks assessments to assess the vulnerabilities and consequences of disruption. Cost estimates for different options for rehabilitation and cost-benefit analysis are conducted at this stage.
- **Information Protection.** Appropriate methods to protect security and physical vulnerability assessments at water and wastewater infrastructure must be implemented in the short term.
- **Short-Term Risk Reduction Implementation.** Address all security gaps and implement mitigation of high risk vulnerabilities in the physical infrastructure.
- **Training.** Training the water utility personnel and their consultants on the security risk assessment methodology are important short-term steps.

B. Intermediate Term Action Plan

- **Infrastructure Rehabilitation.** Continue with the risk reduction implementation to cover all threats to physical infrastructure for an immediate occupancy level and continued operations of critical infrastructure. Detection, assessment and delay elements are to be incorporated around critical assets.
- **Real-Time Monitoring.** This is critical at this stage. Install new monitoring capabilities to detect contaminants throughout the water infrastructure, from source water to continuous monitoring at multiple locations throughout the distribution system. Early warning detection capability in water quality will allow closing water intakes.
- **Implement Redundancy in Water Infrastructure.** These improvements reduce consequences. Single points of failure are avoided with the addition of pipelines, storage tanks or alternate energy sources.
- **Back-Up Systems.** Back-up generators that are designed and installed, or working with the local power supplier, for periods of extended power outage.
- **SCADA Improvements.** Update existing and newer systems to include enhanced security measures.

C. Long Term Solutions

- **Alternative Solutions.** Investigate for applicability and feasibility innovation in the distribution and treatment of potable water. Use of bottled water, point-of-use or point-of-entry treatment, dedicated potable water distribution are among the options that can be implemented for the 1% of production of drinking and cooking water.
- **Reducing Consequences.** Continuing study of vulnerabilities that would affect consumed water and implementing water threats mitigation.
- **Advanced Treatment Technologies.** Mainly for water for drinking and cooking, sophisticated treatment technologies can be implemented for the 1% of production.
- **Distributed Treatments.** Installing localized or community-based systems that provide the final drinking water treatment.
- **Integral Lifelines Protection.** Secure the treated water and wastewater pipelines against natural and intentional threats along the distribution lines.
- **New Standards.** Perform security risk assessments on the water infrastructure on a scheduled basis to help ensure that needed operational and security improvements are reducing risk.
- **Education.** Education for future water infrastructure designers. Security and all-risk assessment courses at BCWWA and APEGBC can be programmed on a regular basis.
CONCLUSIONS

The sources of human-induced security risks to water utilities can include vandals, insiders and past employees, domestic extremists, international terrorists. RAM-W is an excellent security risk assessment methodology that addresses many of the vulnerabilities of the water infrastructure. However, water infrastructure in British Columbia is also subject to additional natural threats such as earthquakes, geotechnical hazards (landslides, liquefaction), severe weather and flooding that can severely disrupt water and wastewater facilities and distribution infrastructure. These risk elements can be both assessed technically and mitigated within an Enterprise Security and Risk Mitigation Plan. ESRMP is an analytical process developed by Stantec Consulting Ltd., which focuses on identifying security gaps and site-specific hazards for managing natural, operational and man-made risks on a defined portfolio of assets and operations. Its application on the water infrastructure of British Columbia would address the complete spectrum of hazards and associated risks such as property risks, operational risks, operational reliability, quality control, and all safety, health and environmental hazards.

REFERENCES

4. Statement of C. Paul Robinson, Director Sandia National Laboratories, U.S. Senate, Committee on Energy and Natural Resources, July 2002
6. “Criteria to Determine Site Criticality”. Peter M. Evans, Stantec Inc. Security Management Services, 2001