Making the Business Case for Utility Security (Adopting an All-Hazards Approach)

John W. McLaughlin

This article describes and offers justification for what is becoming the accepted approach to infrastructure, and specifically utility security. In this article, the term "utility" is defined as any type of water or wastewater agency. The accepted approach referenced here is described as All Hazards. The name implies exactly what it covers: All Hazards. In order to understand the reason for and development of this approach and name, you need to understand the background and history to utility security.

First, a few words of explanation: This article and the assumptions it contains presume a utility has performed a vulnerability analysis or assessment and that the focus here is on the most critical or high-consequence assets, thus limiting the range of assets to be considered raising the relative risk level and improving the cost-benefit results. The ideas and concepts presented are the author's alone and do not necessarily align directly with any specific, current processes or initiatives underway. These ideas and concepts represent the author's belief concerning how to develop and present the business case for security improvements to a utility decision maker.

Prior to the watershed moment known as 9/11, very few utilities had adopted a proactive, holistic approach to security. This was an era when hurricanes and natural disasters dominated concerns about utility security. Emergency response came in to play only when dealing with line breaks, power outages and overflows.

It is likely that a significant number of intentional acts occurred at utilities in the 20 years or so leading up to 9/11, but most were either not reported or certainly not connected to any larger concern. The events of 9/11 changed that thinking dramatically. Suddenly, anything seemed possible and the threat of terrorism changed virtually every utility overnight. This was the era of heavy focus on prevention and threats, as represented by the initial rush of vulnerability assessments (VAs) required by federal law.

The two major methodologies developed in this timeframe were the Risk Assessment Methodology for Water Utilities™ (RAM-W™) and the Vulnerability Self Assessment Tool (VSAT). While both allowed for mitigation or resilience as improvements to reduce risk, the strong focus was on determining the threat and thus preventing an attack (detect, delay, response and deterrence).

Almost forgotten in the rush was the requirement to also develop emergency response plans (ERPs). Utilities were expected to fully develop these plans in under six months and focus on the threats derived from the VA. This rush to complete ERPs coupled with focus on intentional acts naturally reinforced the attention on threats and prevention.

The last few years following that initial rush by water systems to complete VAs have seen a shift in thinking at many utilities. While some utilities proactively have adopted a holistic or All Hazards approach to security, most utilities have not. That immediate concern over a potential large-scale terrorist attack on a water system has faded, and in fact, most utilities don't see the risk as real to them.

Many utilities outside major metropolitan areas have convinced themselves that their only risk is from a terrorist attack, and that the likelihood of such an attack is minimal. This thinking is driven by two factors. First, there is a reality to the idea that the majority of utilities are not likely to be the target of a terrorist attack. Second and maybe more to the point, utilities have so many resource-intensive issues facing them besides security—including regulatory, operational, and financial.

The first argument can be refuted by the idea that the credible and costly threats to a utility go well beyond a terrorist attack. The second argument can be addressed by understanding the multiple benefits gained from a holistic approach. The holistic approach recommended in this article will benefit a utility when it comes to either intentional, accidental, dependency-related, or natural hazards.

In 2005 the National Drinking Water Advisory Committee Water Security Working Groups developed the 14 Elements of an Effective Security Program. These elements have been refined through the Water Sector Specific Plan (SSP) into 10 features of an active, effective protective program.

The SSP is based on the All Hazards concepts and framework established in the National Infrastructure Protection Plan.The features of an active, effective program were developed for drinking water and wastewater utilities (water sector) to help in preventing, detecting, responding to, and recovering from adverse effects of All Hazards, including terrorist attacks and natural disasters.

John W. McLaughlin, P.E., is the manager of the Charlotte, North Carolina office of Jordan, Jones & Goulding, a Jacobs Engineering Group company. This article was presented as a technical paper at the 2009 South Carolina Environmental Conference.

These 10 features are summarized as follows:

1. Integrating protection concepts into culture, leadership and daily operations.
2. Identifying priorities, resources, and measure.
3. Detecting contamination.
4. Assessing and reviewing risks.
5. Controlling access to facilities and information.
6. Incorporating resiliency concepts into physical infrastructure.
7. Assuring continuity of business/service planning and testing.
8. Creating partnerships with peers, interdependencies.
9. Maintaining internal and external communication.
10. Maintaining threat awareness and protocols.

All Hazards Approach

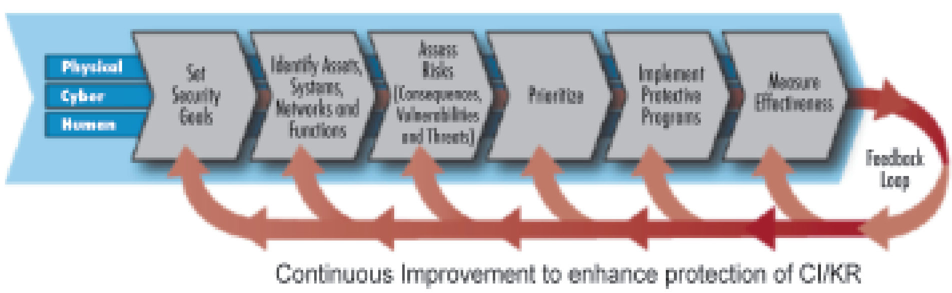
The All Hazards approach is just what it seems: security of a utility where the operational and physical improvements are aimed at providing multiple benefits to the utility. These are benefits to a utility regardless of whether the risk is from an intentional attack, a natural disaster, a dependency hazard, or an accidental event. In such a philosophy, the cause of the event is less important than the effect on the utility.

This same approach also de-emphasizes the importance of the threat. The threat is still important when it comes to prevention of an intentional attack, but that is only a part of a holistic approach to utility security. Response, recovery, and resilience become the major goals.

In 2000, the North Carolina American Water Works Association/Water Environment

Continued on page 26

National Infrastructure Protection Plan Risk Management Framework



High Consequence Asset Susceptible to Multiple Hazards

Continued from page 24

Association formed the Disaster Preparedness Committee. This committee initially focused on how to be better prepared to deal with future disasters in the aftermath of the devastating effects of Hurricane Floyd in 1999. This initial focus proved to be almost prophetic in the way it shaped thinking for the events of 9/11.

The first actions of the committee revolved around what was termed Mutual Aid Disaster Intervention Response Teams (MADIRTs). Within that idea came the concept of Cause vs. Effect. As noted previously, the effect on a utility is more important than the cause. In that concept, the committee developed six core effects:

1. Loss of Access (debris blocking roads, flooding, etc.)
2. Loss of Power (area wide power outage, generator failure, etc.)
3. Chemical Spill (directly or indirectly impacting the utility)
4. Contamination (contamination of water supply or potable water)
5. Water Shortage (through intentional destruction of critical supply facilities or natural events such as drought)
6. Component Failure (due to intentional, natural or accidental cause)

With this concept came the importance of developing resource typing and prearranged teams of trained crews with equipment and parts. This concept has given way to the nationally accepted Water/Wastewater Agency Response Network (WARN), first conceived and practiced in Florida in the aftermath of the hurricanes of 2004 and 2005. The basic idea with WARN was the same as with MADIRT: utilities prepared to help other utilities intrastate and interstate with response and recovery against the effects of a major disaster, regardless of the cause.

The entire concept as currently envisioned, incorporating sensible prevention and the importance of response, recovery, and resilience, is now being incorporated into a process known as Risk Analysis and Management for Critical Asset Protection, or RAMCAP™.

All the above improvements (and many more) fit the mode of providing multiple benefits to a utility and also come into play after prevention has failed. Those multiple benefits come by way of helping whether the hazard is intentional, natural, dependency-related or accidental.

Again, no utility can hope to prevent all possible hazards from impacting them, and with natural, dependency-related or accidental hazards, prevention is virtually impossible. This is the fundamental basis for the focus on the effect of an event versus the cause of an event.

All these improvements are very cost-effective if properly implemented. A word of caution: While the actual dollar cost for all is relatively low, that doesn't mean they are easy to implement. To the contrary, they can be very difficult to implement because they mean a significant change of culture within the utility. That cultural change begins with the key decision makers but must be bought into by all layers of the utility or else they can never be truly effective.

Risk Costs

It is plausible enough to believe that making security improvements within an All Hazards framework is a more cost-effective way to approach security. Theoretically, every dollar spent on improvements benefits the utility relative to four types of hazards (intentional, natural, dependency and accidental). This argument alone should be enough to support making those All Hazards type of improvements.

Understandably, the argument above doesn't always create a strong enough business case to key decision makers for undertaking even the most basic improvements. By definition, a business case is used to determine the financial impact of spending money. In a business case analysis for a security program, the cost of potential improvements, along with the benefit gained, would be weighed against the risk cost of doing nothing. The ability to assign costs to the risks or consequences associated with not doing anything is important.

For the purposes of this high-level look at cost vs. benefit, this article addresses only initial or capital cost and assumes that we are looking at a potable water utility serving a medium-sized community in the United States. Like most utilities, this one is subject to intentional, natural, dependency-related, and accidental hazards. Any number of scenarios could exist but this paper will assume that a critical facility/asset (deemed critical by the previously completed VA) between the water treatment plant and the community served has been damaged/failed.

As already noted, the cause is less important than the effect. This effect falls under Water Shortage and Component Failure. The listing below summarizes the main areas of risk cost or consequence along with the type of impact and of the costs involved.

- ***Replacement Cost***—Because the utility was not prepared in advance with the necessary equipment and replacement parts, the cost paid is a premium and shipping has to be expedited. This does not even account for the time lost in getting the equipment. This time lost will impact the other costs listed below.
  Order of magnitude cost = $10,000 to $50,000
- ***Loss of Revenue (Utility)***—(1) Loss of water service (and loss of revenue to the utility) to at least 20,000 customers; (2) duration of outage, presuming the utility is unprepared to deal with the interruption = five days+; (3) presume lost revenue of $2 per day per residential customer equivalent
  Order of magnitude cost = $200,000+
- ***Loss of Revenue (Community)***—Of the 20,000 customers losing potable water supply, three are deemed critical due to large employment base and/or other significance to the community. Another 100 are small businesses forced to close due to the interruption.
  Order of magnitude cost = $1 million+
- ***Environmental Cost***—This applies more to the wastewater but in the case of a hazardous chemical that might spill as a result of one of the four hazards, the impact on the environment could be significant.

Typical Critical System Facility/Asset

Cleanup alone for a significant spill will run into the thousands of dollars, not to mention the long-term environmental impacts.

Order of magnitude cost = $1 million to $10 million+

- ***Operations Cost***—The cost of additional operational hours used to locate and repair the failure. The additional cost is based on the fact that the utility crews are not trained for or focused on this critical point of failure.

  Order of magnitude cost = $50,000 to $100,000
- ***Cost of Liability***—One of the critical customers is a large hospital where patients are at immediate risk due to potable water shortage. It is clear to the community that this event was serious and that the utility was not well prepared. All this leads to lawsuits and even potential criminal action. The costs include the value of any lawsuit, settled out of court or not, plus legal bills and staff time to defend the case. If deaths are involved as a result (directly or indirectly) of this asset failing, the high end of cost below would be even higher.

  Order of magnitude cost = $1 million to $10 million+
- ***Value of Loss of Public Confidence***—This is perhaps the hardest risk cost to assess accurately; however, this risk can be broken into several related factors and a general order of magnitude can be assumed for each.
  - **Long-term revenue decline**—With a serious event, where it is clear to the community that the utility did not prepare well and was caught off guard, there is a likely long-term loss of credibility about whether the potable water is or will ever again be safe. This leads more and more people to use bottled water, and thus a long-term revenue decline.

    Order of magnitude cost = $100,000s
  - **Difficulty getting financing**—If general obligation bonds are being sought, the community would have to vote for approval; with a serious lack of public confidence over lack of preparedness, an affirmative vote would be in jeopardy. If funding must be approved by a politically elected board, a similar effect would be felt.

    Order of magnitude cost = $100,000s
  - **Utility leadership lose their jobs**—Job loss as a result of the fallout from a utility's lack of preparedness comes with an immediate loss of individual income; however, this is just the tip of the iceberg. Because those impacted are likely to be the key decision makers, reputations and future earning power will be impacted greatly.

    Order of magnitude cost = Immeasurable

The total of all risk costs is between $4 million and over $22 million. Because risk is a factor of both consequence and likelihood, a level of recurrence must be assumed. Each of the four hazards that could lead to the failure carries with it a presumed recurrence.

Because the failure in this scenario could be caused by any of four types of hazards, the combined recurrence (likelihood of the event occurring in a given period of time) is greatly increased. An intentional threat capable of causing failure would not have to be at the terrorist level, thus increasing the likelihood of the event occurring.

A natural disaster capable of causing failure would not have to be a major hurricane. It could be caused by a strong storm, lightening, or other localized event.

A dependency hazard presumes another infrastructure-critical service at this facility fails. The example would be a power failure where no generator exists locally, inability to receive spare parts due to a transportation breakdown, etc.

Finally, an accidental failure is relatively likely since preventive maintenance of this critical asset is presumed to be lacking already and any number of daily events could cause failure.

Improvement Costs

A certain level of prevention is important, but the reasoning behind an All Hazards approach is balancing prevention with response, understanding that no utility can afford to prevent every attack. A summary of the improvement costs is provided below to give an approximate order of magnitude cost.

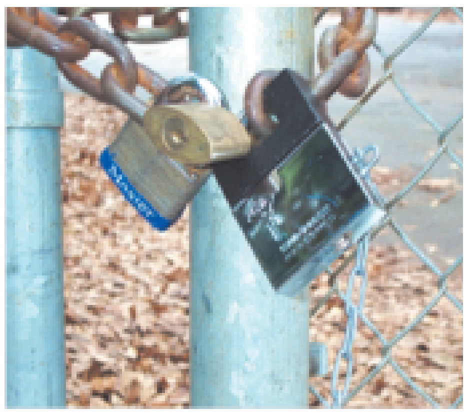
As with the risk cost summary, we are looking at a potable water utility serving a medium sized community in the United States. Again, this one is subject to intentional, natural, dependency and accidental hazards. We will assume that a critical facility/asset (deemed critical by the previously completed VA) between the water treatment plant and the community served has been damaged/failed.

- ***Prevention***—As already noted, a certain level of prevention is necessary, but with the understanding that no utility can prevent a successful attack by a high level threat (or a natural disaster, dependency hazard or accidental event). The ability to reduce the risk from a high-level threat comes from the All Hazards approach and follows the logic that a utility must be prepared to address the effect of an event more than focus on the cause of that event. From the VA, prevention can be broken into three main components: detection, delay, and response (prior to an event occurring). Each of these three components has an operational and physical side.
  - **Detection**—For this example, detection is presumed to incorporate closed-circuit television with image recognition; card access at all entrances; and operational policies and training focused on alarm assessment, enhanced patrols, and staff awareness.

    Order of magnitude cost = $75,000 to $150,000
  - **Delay**—Delay is among the more cost-effective means of prevention. For this example, delay means enhanced fence lines, better locks for all entrance gates, strengthening door locks, bars and grates at critical assets along with operational policies and training-focused key control, access control, and staff awareness.

    Order of magnitude cost = $50,000 to $100,000
  - ***Response (prior to an event occurring)***—Unlike emergency response occurring after an event, this response is aimed at having a response force (police, sheriff, etc.) arrive in time to prevent a successful attack. In this example, this includes the cost of relationship-building with local law enforcement, better communication equipment, and operational policies and training focused on better staff awareness and reaction.

Continued on page 28



Example of Delay Is this Effective?

Continued from page 27

Order of magnitude cost = $1,000 to $10,000

The previous improvements are the ones focused on prevention. In order to better understand the philosophy and benefits of a Cause vs. Effect, or All Hazards approach, a few examples are in order. Each of the following utility improvements provides multiple benefits against multiple events, with an order of magnitude cost given. Again, these are only the initial costs, but the life-cycle costs for maintaining a state of preparedness will be low after the program is initially developed, which is what the costs included here represent.

- ***Emergency Response Planning***—This is fundamental for any utility but is often overlooked as one of the most important elements of an All Hazards approach. In reality, every other piece of an All Hazards resilient plan is part of good emergency response planning. This step was already started with the federal requirement for performing an emergency response plan. The only additional cost is for updating and expanding the plan, but it is presumed that the utility employs an outside consultant for assistance.
  Order of magnitude cost = $50,000 to $100,000
- Critical Asset Determination—This is an integral piece of a VA, but it serves a major function beyond just determining a utility's level of risk. When looking at response, recovery, and resilience as part of an All Hazards approach, understanding where a utility is most vulnerable allows for a focusing of resources, equipment, and training to gain the most benefit. Again, this provides for multiple benefits for the effect of an event, regardless of the cause. Because this improvement has already been included in the VA, there is no additional cost.
  Order of magnitude cost = $0
- ***Prepositioning Critical Replacement Resources/Parts/Equipment***—This improvement goes hand in hand with Critical Asset Determination. The prepositioning of resources, parts, and equipment for the utility's most critical assets allows the utility to respond much quicker and much more effectively. No additional cost is included because this improvement can be achieved with proper management of existing inventory.
  Order of magnitude cost = $0
- ***Crew Training for Rapid Repair of Critical Assets***—As with critical asset determination and prepositioning of resources, parts, and equipment, having a utility's crews well trained for rapid response and repair of critical assets provides benefits from either an intentional, natural, dependency or accidental hazard. The primary cost for this improvement is included in existing staff payroll. Additional costs are included to develop enhanced training programs and for outside training, where needed.
  Order of magnitude cost = $10,000 to $20,000
- ***Business Continuity Planning***—The financial and liability consequences of not having a strong, effective business continuity plan in place may be the greatest a utility can face, but they may also be the most ignored. Imagine the risk cost to a utility if customer records were lost or compromised, if employee files were lost, or if access to physical facilities and all these files were impossible. Because few utilities have truly developed a business continuity plan, the cost for this improvement includes starting from scratch.
  Order of magnitude cost = $30,000 to $50,000
- ***Tabletop and Real-World Exercises***—Exercises, particularly tabletop exercises, designed to truly test a utility and uncover weaknesses are among the most cost-effective improvements a utility can undertake. Any effective exercise should involve multiple layers of staff and result in a failure of the utility to respond effectively. These failures should be identified in a "hot wash" follow-up discussion and lead to specific action items. The next series of exercises should be more and more difficult and should focus on high-consequence events, regardless of whether they are caused by intentional, natural, dependency-related, or accidental hazards. The cost for this improvement presumes that the utility employs an outside consultant.
  Order of magnitude cost = $10,000
- ***WARN Membership***—The Water/Wastewater Agency Response Network or WARN was created about three years ago. WARN is a network of utilities helping utilities during preparedness, response and recovery from a small, large or catastrophic emergency. Programs include the use of a mutual aid and assistance agreement that allows utilities to cross jurisdictional boundaries to provide aid during and following an emergency. Participation is voluntary; there is no obligation to respond. The cost for this improvement is minimal, since most costs are reimbursable for a major event.
  Order of magnitude cost = $0
- ***Relationships with Local First Responders***—This is a low-cost improvement that carries huge potential for benefit. The old adage is as true now as it has ever been: The time to get to know your local first responders is NOT at the scene of an event. Getting to know local first responders (police, fire, rescue, HAZMAT, etc.) can be as simple as an occasional lunch or other meeting, offering access and tours of utility facilities, or participating in area-wide tabletop and real-world exercises. With the requirement that all utilities be trained in Incident Command System and the National Incident Management System, a relationship almost becomes mandatory as a result. This improvement carries very low cost (lunches, food, etc.); primarily it involves time spent developing the relationships.
  Order of magnitude cost = $500 to $1,000

The total of all improvement costs is between $230,000 and $440,000. Even in a conservative assessment, the risk costs are 15 to 40 times higher than the improvement costs. Referring back to the paragraph which describes the likelihood or recurrence of the four hazards being considered as causes, can any utility feel confident that this type of event will not occur in 15 to 40 years or more?

Even if utility officials can convince themselves that statistically this event will not occur in over 40 years, how much is a life worth, what is the value of the reputations of key utility staff, the cost of a careers lost, and the value of the public confidence built up over years of safe, reliable service?

Water vs. Wastewater

A similar dollar case can be made for a wastewater scenario. In a similar wastewater scenario, the risk costs for replacement, loss of revenue (utility and community), and operations would be along the same order of magnitude as a water utility because without service available, these costs will rise.

The liability and value of the loss of public confidence might be lower for a wastewater scenario vs. a water scenario because of the lower potential of loss of life and the lower public concern over wastewater as opposed to water. The environmental cost will be significantly higher for a wastewater scenario because of the potential for hazardous chemicals being released and the almost certain large sewer spills into the environment to be expected.

Regardless of the hazard, developing improvements with multiple benefits that lead to a resilient utility system will be multiple times more cost-effective than doing nothing and relying on the likelihood of any one of the four types of hazards never occurring at your utility.

Conclusions

It has been said that security for utilities should be integrated into the culture of a utility, much like safety has over the last 20 years. This means that security is an integral part of the utility, at all layers in all aspects.

These changes need not be excessively costly in pure dollar terms, but even when dollar cost is involved, compared to the risk cost; the decision to make these improvements should be easy. A well-run utility is a secure utility.