

Protecting our Water Infrastructure



After the September 11 terrorist attacks on the U.S., state and federal officials launched a number of initiatives to protect the country from any future attacks. As part of that effort, public officials and citizens began to pay close attention to whether our nation's infrastructure, including its public water supply systems, are secure from terrorist and other threats.

Congress quickly adopted legislation requiring water utilities to conduct vulnerability assessments to evaluate a system's susceptibility to potential threats and identify corrective actions. States were also urged to adopt laws to protect assessments and other information which could jeopardize the security of water supplies, treatment centers, transmission, and distribution systems from disclosure under freedom of information laws.

It's been ten years since 9/11 and Osama Bin Laden is dead. Are potential terrorist attacks still a threat to our public water supplies and other infrastructure?

Unfortunately, yes.

Recent incidents continue to demonstrate that the nation's public water supplies are vulnerable to attack not just by Al Qaeda and affiliated groups but by other organizations and individuals.

Simon J. Stringer, Chief Executive & Managing Director of Becatech Inc. a firm specializing in protective security technologies, spoke at the CWWA/CTAWWA Fall Conference on this issue. He highlighted the following recent incidents as evidence that threats to our public water supplies persist, including:

- Al – Awlaki - Specifically sought to use poisons (Ricin and Hydrogen Cyanide) to attack USA and the United Kingdom
- San Antonio Water Authority – Suspected terrorists were recently arrested with photographs and maps of water systems and other infrastructure
- Perth Australia – Activists were arrested scouting water tanks and pipelines

As Stringer noted, however, concerns over the potential for water-related military or terrorist action are not new. As far back as the first century, C.E., Nero used cherry laurel water, which contains cyanide, to

poison the wells of his enemies in ancient Rome. And in 1941, J. Edgar Hoover, director of the Federal Bureau of Investigation, acknowledged that “water supply facilities offer a particularly vulnerable point of attack to the foreign agent due to the strategic position they occupy in keeping the wheels of industry turning and in preserving the health and morale of the American populace.”

Political or ideological terrorists, vandals, disgruntled employees or former employees and lone criminals have long posed a threat to national infrastructure. “And water is one of the most vulnerable in terms of denial of service and loss of life – 5,000 gallons of industrial hydrogen cyanide will poison approximately 300 million gallons of treated drinking water. Other chemicals are even more lethal,” Stringer said. “In addition, the organization and resources required to launch an attack is not complex or expensive.”

What has changed, Stringer points out, is the intent, the lethality and the sophistication of threats to our systems. “Terrorism is now unconstrained and coupled with the desire to commit mass murder. The increased use of suicide attackers and the availability of more sophisticated and lethal weaponry, including, chemical, biological radiological and even possibly nuclear weapons, has heightened the need for protective security measures.”

“Unfortunately, the analysis suggests that terrorist related events are expected to increase over the next two decades. And history suggests that attacks will move from the spectacular – aimed at iconic national landmarks – to targets that are harder to defend and that are more disruptive and destabilizing to the public,” said Stringer.

Protecting national infrastructure poses significant challenges. By nature and design, it is dispersed across the country in a way that prevents the whole infrastructure from being protected from attack. It is therefore necessary to protect the most vulnerable and critical elements of the infrastructure. “The attack cannot be prevented but it can be detected. The issue is

Continued on page 18

Protecting our Water Infrastructure

therefore to ensure that an attack is detected in time to allow corrective action to be taken,” Stringer said.

What’s troubling, however, is that despite the increased threat of terrorism, companies are investing, somewhat blindly, in CCTV, Entry/Access Control, commercial firewalls and software, Emergency Responses and Resilience based security – technologies that are very good at telling you what happened after the fact but absolutely no help in protecting you from attack, Stringer said.

What can we do to protect our infrastructure?

Although state and federal agencies have initiated numerous programs to better protect the nation’s infrastructure, according to a recent report, The Biological Threat to U.S. Water Supplies: Toward a National Water Security Policy, “the current strategy to secure national water supplies places the bulk of the responsibility on individual utilities...”

Stringer points out that utilities should therefore get serious about developing and integrating into their systems protective, layered security measures by:

- 1) Undertaking meaningful vulnerability & risk assessments;
- 2) Optimizing concepts of operation and responses;
- 3) Training against/exercising against meaningful scenarios;
- 4) Understanding the concept of layers of security not protective security; and
- 5) Undertaking thorough Political, Economic, Social, and Technological analysis (PEST Analysis).

Stringer also pointed out that efforts to enhance security cannot be one-size-fits-all. They must be impact-led, vulnerability-focused and threat-informed. He also suggested that water utilities take the following steps:

- All employees and contractors must be vetted/ background checked. There are several incidents where disgruntled employees or former employees attempted to tamper with water infrastructure or supply
- Systems must provide early detection of the actions of terrorists, criminals and other intruders in sufficient time and at sufficient distance from a target to leave enough time for something to be done
- Systems must encompass proven and reliable technology and protocols. False alarms are unacceptable
- Systems must provide layers of security – Stand Off capability

- The systems themselves must be protected, self-powered, and resilient.
- Systems must integrate into existing infrastructure and concepts of operation
- They cannot be of the “In Emergency Break Glass” design
- People must train what to do and how to use these systems all the time

Unfortunately, Stringer said, “History is littered with examples of where this was not done, including the BP Oil spill in the Mexican Gulf, the attacks on hotels in Mumbai and the 7/7 attacks in London.”

Stringer’s firm, Becatech Inc. offers utilities enhanced security systems designed to protect access to water treatment facilities, water pumping stations, storage facilities and buildings by using modern sensor and intruder detection technologies. This system, Becatech Watercross®, provides a wide range of sensors from basic hatch to sophisticated sensors such as vibration and acoustic. The alarm can be interrogated either via transmitted mobile number or via a satellite link which will trigger a message that will confirm the site name, the point of attack and the type of sensor that has been activated.

Other companies also offer intrusion detection systems to protect access points in drinking water distribution systems against the threat of intentional contamination. Unfortunately, a recent report by the Government Accountability Office indicates that water utilities face certain obstacles in enhancing security measures. Not surprisingly, utilities cited the cost of upgrading security as a major obstacle because they are also struggling to upgrade water distribution infrastructure and treatment facilities.

Unfortunately, federal and state homeland security grants are typically used up by first responders and many water utilities are facing significant pressure from state regulators and municipalities to hold down rate increases. Although Congress continues to consider legislation to target funds to assist utilities in upgrading water infrastructure and security, the legislation has taken a back seat to other priorities.

Simon J. Stringer, Chief Executive & Managing Director of Becatech Inc., can be reached at ssstringer@becatech.com 