ASA

Risk Consultants

Research Note

Risk and the Water Sector

By: Ilya Krivulin

Keywords: water sector, operational risk, HSPD, CIKR

Abstract – The Water Sector is one of the eighteen critical infrastructure sectors identified by the Department of Homeland Security. This research note identifies potential operational risks associated with the sector, the impact those risks create, provides real life examples of operational breaches and explains why this particular sector just might be the most important of the eighteen.

Introduction

The Homeland Security Presidential Directive-7 (HSPD) has identified eighteen critical infrastructure and key resources (CIKR) sectors that are critical in maintaining the country's infrastructure in terms of day-to-day operations, viability and economic sustainability, and described the ways to protect these sectors from terrorist attacks and other hazards in sector (and context) specific plans in support of the risk management framework called National Infrastructure Protection Plan (NIPP). This research note will focus on the Water Sector. It will identify the sector "assets" and the potential operational risks associated with those assets on the government side, extend the discussion about risks and vulnerabilities into the private sector, provide real-life examples of operational breach and conclude with a few recommendations for further mitigation of the risks discussed.

Why Water Sector?

Historically, water has been an integral part of human existence: simply put, humans physically cannot survive without an uninterrupted supply of clean drinking water. The proper treatment and disposal of wastewater is also critical in prevention of disease and contamination. Both of these types of water – drinking and wastewater – comprise the Water Sector. "There are approximately 160,000 public drinking water

systems and more than 16,000 publicly owned wastewater treatment systems in the United States. Approximately 84% of the U.S. population receives their potable water from these drinking water systems and more than 75% of the U.S. population has its sanitary sewerage treated by these wastewater systems."[1]

Alongside individual consumption, we also have to keep in mind such important organizations as hospitals, educational facilities (i.e. schools and universities), airports, stadiums and arenas, large event venues, firefighting equipment (like fire hydrants) – all of which are highly dependent on an uncontaminated water supply and proper disposal. All our communications with the rest of the world may be cut out in the case of a major cyber security breach, we may spend many nights in darkness and cold as a result of a major power outage, we can last without food for quite a few days before our body gives in, but without water we will not survive even for 48 hours. In addition to this, research shows that the water sector, despite having a rich history of water quality monitoring under guidance of Safe Water Drinking Act (SDWA) and Clean Water Act (CWA),[2] is not an area that was built with security in mind in comparison to energy and nuclear sectors, for instance.[3]

Who Is in Charge?

The HSPD-7 has designated the Environmental Protection Agency (EPA) as the body responsible for establishing various programs that support "security-related activities, with the goal of enhancing the Water Sector's ability to plan for and respond effectively to security threats and breaches."[4] It is important to note here that the NIPP relies on partnerships and extensive communication between the members of those partnerships in achieving the framework's goals of maintaining a secure and uninterruptable national infrastructure. Taken from a 2010 EPA report, [5] below is the summary of EPA's responsibilities and information about its partners.

- EPA handles the receipt of community water systems vulnerability assessments (VAs) and emergency response plan (ERP) certifications.
- The Water Security Initiative (WSI), the Active and Effective Security Program and the Water laboratory Alliance (WLA) programs work towards aiding the Water Sector in maintaining public health and protecting the environment.
- Department of Homeland Security (DHS) is a supervising partner in recognizing and reducing risks through risk assessments in the sector.

- Information Sharing and Analysis Center allows for gathering, analyzing and disseminating threat information specific to the sector.
- In order to enhance preparedness and response, the Water/Wastewater Agency Response Networks (WARNs) are established.
- In order to maintain a resilient infrastructure, a series of training exercises and drills in support of National Incident Management Systems/Incident Command System (NIMS/ICS) is conducted to help the Water Sector utilities to have better communication and incident response.
- EPA also partners with public and private utilities, national Water Sector associations, States, Water Sector Coordinating Council and the Government Coordinating Council to further enhance cooperation and security amongst Water Sector utilities.

What Is in the Systems?

Next it is appropriate to introduce the components of water systems (this research note will focus on drinking water) and to identify sample assets and electronic systems in the Water Sector. The reason for enumerating these is that the security breach can happen to any of the

components listed below, thus increasing EPA's range of responsibilities towards mitigating risks. Depending on the size of the utility the components may include all or some of the following[2]:

- Water Source (ground or surface)
- Conveyance – from a remote source to a treatment plant
- Raw water storage – reservoirs or lakes in remote or urban areas
- Treatment – physical and chemical, depending on contaminants detected in raw water
- Finished water storage – before distributing to customers;
- Distribution system
- Monitoring system – this one is of utmost importance as monitoring provides visibility into what needs change or upgrade in the controlling equipment as well as presents a potential security threat had the monitoring data, like the consistency of contaminants for example, leaked into malicious hands.
- Supervisory Control and Data Acquisition (SCADA) system – linkage (often wireless) between various components of the monitoring systems in order to provide necessary data or automate operations at a facility.

An "asset" in the Water Sector is defined to be "an entire system for purposes of identification, prioritization and coordination."[6] Utilities are

expected to run risk assessments of their own on each of the key components and assets that, if affected maliciously, will have negative effects on operations within and outside the sector. In addition to SCADA, the Water Sector cyber security infrastructure includes the following[7] assets:

- Central control station
- Human-machine interface
- Local processes, instruments and operating equipment
- Workforce – lack of appropriately trained personnel may result in inability to carry out necessary operations and provide services to the customers.

Lastly, it is important to note that such databases as Safe Drinking Water Information System (SDWIS) contain very sensitive information, like complete inventories of Public Water Systems, water sources and detailed location and treatment information and therefore present a potential security threat. We have now laid the foundation to discuss the risks and impacts in the Water Sector.

Risks and Impacts

As we saw above, the ground for risks in the Water Sector is vast and the occurrence of such may directly affect other sectors due to interconnectedness. The first and most obvious risk is the infection of

public health due to agent contamination, release of poisonous gas, or any other malicious means of making water unusable. The extent of the impact will vary depending on how fast the problem gets discovered and how dense the population is in the area of the incident. Since contamination can spread through more than just one way, like inhalation, ingestion or skin absorption, the impact from drinking or otherwise consuming unusable water can be huge.[8] It is important to keep in mind that a diseased population means reduced workforce numbers, thus the productivity may have a cascading diminishing effect on the economy. Closure of businesses, school and restaurants are all examples of an economic impact. Next in mind comes the question about the infrastructure recovery: how long does it take to recover a broken utility and what happens when the systems inside that utility are customized and cannot be fixed by readily available equipment? Lastly, the psychological effect may be quite damaging. Even if the contamination does not result in many deaths, it may be quite arduous for governments to restore people's confidence, maintain order and provide basic services while determining the cause of the incident and dealing with decontamination.[9]

Another very curious risk is cyber-attacks. Just like electrical power plants, water utilities are often controlled and monitored by some kind

of a computer system, or in particular, a SCADA system discussed above. An example of such breach would be a recent attack on South Houston's water utility. The attack is believed to have come from Russia and the hacker obtained and publicly posted the screenshots of the utility control system that he claims to have gained access to in almost no time.[10] The hacker stated,

> *I dislike, immensely, how the DHS tend to downplay how absolutely (expletive deleted) the state of national infrastructure is. I've also seen various people doubt the possibility of an attack like this could be done. So, y'know … the city of South Houston has a really insecure system. Wanna see? I know ya do. I'm not going to expose the details of the box. No damage was done to any of the machinery; I don't really like mindless vandalism. It's stupid and silly. On the other hand, so is connecting interfaces to your SCADA machinery to the Internet. I wouldn't even call this a hack, either, just to say. This required almost no skill and could be reproduced by a two year old with a basic knowledge of Simatic."*[11]

He brings up an interesting point of having the system connected to the outside Internet. As long as your Ethernet switches accept traffic from the outside, it creates an enormous potential for malicious

intrusion and thus increases the amount of protection needed for such systems.

Another example comes from Los Angeles, where a local water utility decided to conduct a "pilot" study on the system's security potential. A few volunteers were recruited to try and break the system (this testing technique is known to be used by companies in other sectors, like IBM in information technology). It was reported that within two hours, the testers gained full control of the system without any (!) insider guidance, which would allow them to dump chemicals into LA River making water toxic, while turning off the sensor to detect that.[12] Some other common hazards include:[13]

- Improvised explosive devises
- Vehicle-born explosive devices
- Explosive devices in wastewater collection systems
- Radiological or biological contamination in drinking water distribution systems
- Assault
- Sabotage of water treatment systems
- And of course natural disasters, like earthquakes and hurricanes cannot be overlooked.

Lastly, the importance of interconnectedness of the Water Sector with the other areas should be reiterated. For example, an occurrence of any of the above risks may halt operations of a power generation plant as it may rely on water for cooling. And vice versa, a water utility may come to a halt as a result of interrupted power supply as the utility control and operation systems may be run, monitored and controlled by a computer system.

Risk Assessment

Risks threats come from many different directions: whether it is a terrorist attack, a human mistake, or a computer malicious virus, the water utilities need to be ready to respond in a timely manner. Next, a set of risk assessment initiatives and tools will be discussed, that the private sector currently undertakes and uses to reduce vulnerabilities and enhance preparedness.

As mentioned above, EPA partners closely with DHS to come up with risk assessment documents and tools in order to assist owners and operators in conducting local assessments and making sure that the methodologies are always up-to-date. The EPA have drafted numerous threat documents and holds workshops on raising awareness about various types of risks as well as DHS conducts SCADA educational workshops as part of their cyber security roadmap. The following three

tools are the main instruments of risk assessment in the Water Sector at the present day:[14]

- Risk Assessment Methodology – Water (RAM-W)
- Security and Environmental Management System (SEMS) emergency response checklist
- Vulnerability Self-Assessment Tool (VSAT).

Another example of the government's assistance to the private sector is the non-profit program called LIGHTS. It is a programmatic solution that helps a number of smaller industries, including the Water Sector, to establish the level of cyber security needed in the current conditions. The solution expands visibility into systems, keeps it as cost effective as possible and encourages participation from more communities around the country and even the world. It allows for sharing of anonymized metadata, "at member's discretion, to assist in efforts to increase the safety and reliability of our national infrastructure."[15] It also works with analysis centers to improve situational awareness.

There are many more examples of risk assessment initiatives. It also seems that the government has got a good grip on the issue of having to closely monitor and mitigate risks associated with various critical sectors of the infrastructure and created documents and tools to lead

such initiatives. The government's responsibility toward the private sector is to outreach and educate as much as possible, since the local risk assessment is on the shoulders of the utilities. The threats, vulnerabilities, risks and impact analysis is a complicated process that requires professionals to carry out such duties and make our infrastructure safer. Educational institutions should encourage their students interested in risk management to consider working for one of the sectors in the government instead of pursuing less meaningful consulting in private firms.

Another recommendation is to know the features of your system. During one of the cyber security breaches, it was identified that the intrusion happened not because the system had some kind of vulnerability or a bug, but rather a sheer fact that there were certain features enabled that the customer did not even know about.[16] Customers, i.e. utilities, should take responsibility in learning the systems that they purchase and vendors should be obliged to provide training upon demand.

Conclusion

This research note clearly showed the importance of the Water Sector to the national infrastructure. The CEO of Trusted Metrics,

Michael Menefee, stated that if it was decided that the Water Sector was the most important one, then 12, 24, 36 months won't be enough to get things done. [17] Both the government and private sectors need to continue to closely collaborate with each other to increase protection levels of our water supply facilities. In addition, vendors need to ensure they design the utility assets with security in mind.

References

[1] "Water Sector Snapshot." *DHS.* 2009. Web. 28 May 2012. <http://www.dhs.gov/files/programs/gc_1188399291279.shtm>
[2] "Water Sector-Specific Plan. An Annex to the National Infrastructure Protection Plan." *DHS.* 2010. Web. 1 June 2012. <http://www.dhs.gov/xlibrary/assets/nipp-ssp-water-2010.pdf>
[3] Menefee, Michael. "Cybersecurity in Waste Water and Water Control Systems." 2011. Web. 2 June 2012. <http://www.infosecisland.com/videos-view/18705-Cybersecurity-in-Waste-Water-and-Water-Control-Systems.html>
[4] "Water Sector-Specific Plan.", p. 12.
[5] "Water Sector Snapshot.", p. 2.
[6] "Water Sector-Specific Plan.", p. 19.
[7] "Water Sector-Specific Plan.", p. 20.
[8] "Water Sector-Specific Plan.", p. 24.
[9] "Water Sector-Specific Plan.", p. 25.
[10] Menefee, n. pag.
[11] Byers, Eric. "SCADA Security Breached at U.S. Water Utilities." 21 November 2011. Web. 26 May 2012. <http://www.tofinosecurity.com/blog/scada-security-breached-us-water-utilities>
[12] Menefee, n. pag.
[13] "Water Sector-Specific Plan.", p. 26.
[14] "Water Sector-Specific Plan.", p. 27.
[15] *LIGHTS*. 2012. Web. 27 May 2012. <http://lights.energysec.org/>
[16] Menefee, n. pag.
[17] Menefee, n. pag.