ASA

Annie Searle & Associates LLC

Research Note

Dam Operational Risk

Iisaaksiichaa Ross Braine

May 2016

Abstract: The purpose of this examination of the U.S. Dams Sector was to identify potential control failures and identify the best path for mitigation, specifically in terms of energy. The author used internal audits of the Homeland Security system, combined with best practices pulled from both the "Dams Sector-Specific Plan" and "Operational Risk Management" written by Philippa X. Girling. Findings show that the dams sector has a multitude of process and system exposures with some identified remedies and clear steps leadership can take to strengthen their sector. At the end of this paper, the author discusses potential solutions and illustrates the steps the Dams Sector could take in order to shore up cyber defenses.

Introduction

The purpose of this paper is to identify and discuss one of the sixteen critical infrastructure sector[i] identified by the Department of Homeland Security.[1] Since many of the sectors identified are interdependent, this paper will touch on two closely related sectors. The main sector identified and discussed is the Dams Sector in regards to dam ability as electricity producers, which also affects the Energy Sector.

I have spent all my years either fishing or visiting dams throughout the western U.S. and thought that it was surprising to find that the "Dams Sector" was listed on the official website of the Department of Homeland Security. This should not have been surprising since these large structures are very visible, hold back large volumes of water, produce low cost amounts of energy, and are consistently in the media. I was very interested in the removal of the Elwha and Glines Canyon Dams as a scientific experiment and as an insider to the workings of the process.

[i] Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, and Water and Wastewater Systems

For those who are unware of the project, the Elwha and Glines Canyon dams were built by private companies in the early 1900s to produce electricity. In 2000, the U.S. Department of the Interior, Bureau of Reclamation purchased them for removal. The two dams produced about 40 percent of the energy requirements for the Diashowa American paper mill in Port Angeles.[2] With the removal of the dams, there is a restored salmon run and a loss of electrical production in the area.

This is an exciting subject to write about, because I find the infrastructure of the U.S. intriguing, especially with the increased risk of online security. This paper will aim to discuss a few of the physical and technological operational risks of the Dams Sector in both the government and private sectors along the Columbia River in Washington and Oregon.

Background

The Department of Homeland Security "Dams Sector compromises dam projects, navigation locks, levees, hurricane barriers, mine tailings, impoundments, and other similar water retention and or control facilities."[3] According to the Dams Sector overview, the "sector is a vital part of the nation's infrastructure and provides a wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, wildlife habitat, waste management, flood control, and recreation."[4] In addition, of the roughly 87,000 dams, approximately 65 percent are privately owned and state dams' safety offices regulate more than 77 percent.

Along the mainstream of the Columbia River, there are 11 dams that are both governmentally and privately held as illustrated in Table 1.[5]

Table 1: Dams along Mainstream of the Columbia River

Dam Name	Owner
Grand Coulee	U.S. Department of the Interior, Bureau of Reclamation
Chief Joseph	U.S. Army Corps of Engineers
Wells	Douglas County Public Utility District
Rocky Reach	Chelan County Public Utility District
Rock Island	Chelan County Public Utility District
Wanapum	Grant County Public Utility District
Priest Rapids	Grant County Public Utility District
McNary	U.S. Army Corps of Engineers
John Day	U.S. Army Corps of Engineers
The Dalles	U.S. Army Corps of Engineers
Bonneville	U.S. Army Corps of Engineers

Table 1 is very clear on who the U.S. owners are, however, the Public Utility Districts (PUDs) are not that clear. PUDs are nonprofit, community-owned and governed held utilities that pay bondholders and investors who vote on policy much like stockholders in a private corporation. Grant County PUD is managed by "a five-member board of commissioners made up of local citizens elected on a nonpartisan basis by the people of Grant County. Commissioners set policy,

review operations and approve budget expenditures."[6] In essence, these PUDs are private corporations who own dams and sell the electricity for income.

Key Risks

According to the Dams Sector-Specific Plan, Annex to the National Infrastructure Protection Plan created by the U.S. Department of Homeland Security, "from the security perspective, risk is defined as a function of three parameters: (1) threat, the likelihood of an attack being attempted against a target, (2) vulnerability, the susceptibility of a target to being compromised by an attack, and (3) consequence, the set of undesirable impacts of the attack, if successful."[7]

According to Girling, there are seven operational risk events categories: 1) Internal Fraud, 2) External Fraud, 3) Employment Practices and Workplace Safety, 4) Clients, Products, and Business Practices, 5) Damage to Physical Assets, 6) Business Disruption and System Failures, 7) Execution, Delivery, and Process Management.[8]

I was granted an interview with a high level person in the U.S. Bureau of Reclamation and that person told me there 3 threats that the bureau has identified and they include hacking, infrastructural shutdown, and terror threats.[9]

Hacking is the buzzword of the moment, especially with the large public issues in Target and Home Depot. Users are scared to have their personal information stolen and with current high-speed media, it is a constant scare factor in the news reports. Hacking in the dams sector can cause more than just user information lost, it can result in loss of life. Dams have a modern program called STADA, which is a computerized remote control system. Dams use this system because they have to be constantly adjusted because of demands on power, both high usage as well as low usage. The problem with this remote access is that there is a way for hackers to get into the system and destroy the facility. One worry is that the turbines could be overspun which would cause them to burn out and shutdown permanently. There was one large virus that the Israelis and Americans used to over-spin the centrifuges in Iran and that virus is Stuxnet. The fact that we have used a virus to destroy the capabilities of a fifth of Iran's nuclear centrifuges shows that this threat is very real and very possible. Other things that hackers could hijack are the gates. The gates are what hold the water back and where the water flows when there is a need for more electricity, more water downstream, or to lower the reservoirs. If a hacker was able to open the gates completely, the consequences would be severe as town and cities would be flooded and electricity would cut off.

Infrastructural shutdowns are also a major risk in the dams sector. When a power plant loses all the energy and goes empty, it takes energy to restart the whole system. The only power plants that can start on their own are hydroelectric plants. "In the northwest, Grand Coulee Dam is the largest single generation station and is the single most important power structure."[10] It would be the only plant that could restart any of the other plants in the whole northwest. In fact, it is so valuable and integral to the northwest that it is the only dam with a dedicated armed security force on site and on call at all times. Now that generation has been discussed, there needs to be some time taken to talk about transmission of all this energy. In order to make sure that the

power is flowing to users, there is one commission that monitors all the power generation and transmission and that is the North American Electric Reliability Corporation – Western Electricity Coordination Council (NERC-WECC). The NERC-WECC enforces reliability with audits and establishes standards for both federal and non-federally run dams. The attempt is to reduce the risk of operation errors and show the threat if a dam is not in compliance. The danger in noncompliance is that the system could fail.

Finally, terror threats to the dams sector. While hacking could be done by terrorists, some of them are also done by lone wolf individuals or groups. Not every hacking threat is due to terrorism; sometimes hackers see the system as a challenge and do it just for the thrill. Terror threats in this paper address physical damage to property. If a terror group were to disable or destroy a dam, there would be a ripple effect throughout the sector and region. For example, if the Grand Coulee Dam was to be destroyed, the power created by it would end, floods would destroy homes, and crops would fail. The power created by Grand Coulee produces enough electricity to light 2.3 million homes and serves as the main factor in controlling floods on the Columbia River.[11] Needless to say, it seems that the Grand Coulee is in fact the single most important structure along the Columbia and in the northwest. As I interviewed the executive in the Bureau, I was unable to get how many individuals are in the protective unit stationed at the site due to homeland security directives. These individuals are trained in anti-terror methods and are fully capable of protecting the site for an extended period of time. Again, this is the only dam in the northwest with a fully dedicated armed security force, which makes me wonder how we protect those other dams along the Columbia and throughout the U.S.

Recommendations

Now that the Key Risks have been identified using the Dams Sector-Specific Plan, Annex to the National Infrastructure Protection Plan created by the U.S. Department of Homeland Security of threat, vulnerability, and consequence as well as interviewing the high-level executive, there are some recommendations to create a plan.

First, upon reviewing the Dams Sector-Specific Plan, it is very clear that the teams have created a very comprehensive plan with multiple guides and handbooks. The plan also talks about the cost-benefit plan to determine how much money to invest in a certain aspect and acknowledges that there is not a one-size-fits-all program. My recommendations are based on what I did not clearly see in the 136-page plan.

Threat

The news outlets would make it seem that we are under constant attack and after taking the IMT 556 class in the University of Washington (UW) Information School, these threats seem very real. The biggest revelation was the visit from the Chief Information Security Officer to the UW. He told us that there are constant threats to the security of the UW and if there is that much trouble at the UW, I can only imagine what other threats there are to our other infrastructures.

The best recommendation that I can make on this subject is to hire more people to work in the

security office. We need to hire the best of the best in order to keep the security intact and keep us moving forward. However, there is a huge shortage of security specialists and we need to start training more folks. Universities and the government need to collaborate and start more internet security programs like the one current running in the UW iSchool.

Vulnerability

It is very scary how vulnerable the dams sector truly is. According to a Business Insider article, more than 500,000 potentials targets were identified in power plant systems, water treatment centers, and traffic controls.[12]

As stated earlier in the paper, the Stuxnet virus was able to successfully destroy one fifth of Iran's nuclear power sector. The virus was entered into the system with a minor thumb drive and was able to replicate throughout the system. A second version of the virus was added later and it was only then that it was discovered, however, much of the damage was already done. The Business Insider article showed that whenever an employee sets up a wireless access point to connect to the system without encryption, there is a huge infrastructure exposure.

In order to ease some of this exposure, I would recommend that the networks require encryption and not allow non-recognized users to connect. This is not a popular suggestion since we all need our connectivity to run our smartphones, tablets, and laptops but this practice must be exercised throughout the dams sector.

Consequences

The consequences of a total shutdown in the Grand Coulee dam power plant alone would be a major hit to the northwest and would ripple throughout the region. If the electricity was to cut off, there would be over 2.3 million homes affected and the northwest would be unable to restart any other power plants because of the amount of energy required to restart systems. The same would be said if the turbines were turned on full force and overspun causing them to break down. If the infrastructure was not ready for this major power surge, there would be a blackout and most of the system would be fried.

The consequences if the dam was to be destroyed physically would be the same as above with blackouts and the flooding below the dam would drown many towns and potentially destroy crops who rely on the irrigation system connected to the Columbia River project.

Conclusion

Like most issues in the government and private sectors, money is always at the front of every conversation. Currently, the government is not spending enough money to train security officers at a high enough rate and the income levels are lower than those offers in the private sector. The government needs to make sure that cybersecurity is on the list as an "electronic WMD" in order for it to get the attention that it must have and maintain higher levels of funding.

It appears that the commissions and committee have done an exhaustive review of the processes in the Dams Sector-Specific Plan. If I were to compare this plan to what I have learned in the

IMT 556 class, I would consider this a Risk and Control Self-Assessment (RCSA). A well-designed RCSA program provides insight into risk that exist in the firm, regardless of whether they have occurred before."[13] However, the fact that we still have these vulnerabilities is shocking and eye opening. The government and private dams need to work together with universities to train security specialists. This means more funds, more outreach, and more transparency to the issues, especially the fact that we are so open to attack.

I believe that senior leadership for both government and private businesses need to take the handbooks very seriously and create a mitigation plan for every aspect of their sector. The teams that put together the Dams Sector-Specific Plan was made up of both government and private sector representatives and so this plan works across sectors. However, with most sectors, there is not a one-size-fits-all approach and to leaders need to figure out how they plan to implement this plan. The NERC guidelines help the groups make those better-informed decisions and people like the person I interviewed truly believe in this sector and should be supported.

This sector is so vastly important to the infrastructure of the US and it needs to buff up its security measures and protection. The biggest threat appears to be online activity, we need to have more security officers, and I am hopeful that more people realize the importance of the Dams Sector, I certainly have.

---

[1] "Critical Infrastructure Sectors." Department of Homeland Security. 2014. Accessed Mar. 2015 <www.dhs.gov>.

[2] "Elwha and Glines Canyon Dams, Elwha River near Port Angeles, Washington." Bureau of Reclamation, U.S. Department of Interior. N.D. Accessed Mar. 2015 <www.usbr.gov>.

[3] "Critical Infrastructure Sectors."

[4] "Dams Sector." U.S. Department of Homeland Security. N.D. Accessed Mar. 2015 <www.dhs.gov>.

[5] Confidential Interview with US. Bureau of Reclamation, conducted by Ross Braine. Mar. 2015.

[6] "What is a PUD?" Public Utility District No. 2 of Grant County, Washington. N.D. Accessed Mar. 2015 <www.grantpud.org>.

[7] Dams Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan. U.S. Department of Homeland Security. 2010. Accessed Mar. 2015 <www.dhs.gov>.

[8] Girling, Philippa X. *Operational Risk Management: A Complete Guide to a Successful Operational Risk Framework.* Oct. 2013. Wiley.

[9] Confidential Interview.

[10] Ibid.

[11] "Grand Coulee Dam Statistics and Facts." Bureau of Reclamation, U.S. Department of the Interior. Mar. 2015 Accessed Mar. 2015 <www.usbr.gov>.

[12] Ingersoll, Georffrey and Michael B. Kelley. "There's Only One Thing Stopping Enemy Nations From Smashing America's Power Grid." *Business Insider*. 1 Mar. 2013. Accessed Mar. 2015 <www.businessinsider.com>.

[13] Girling, Philippa.