ASA

Annie Searle & Associates LLC

Research Note

Energy Sector Risk Assessment

Colin Andrade

February 2017

Keywords: Energy Sector; Critical Infrastructure; Risk Assessment

Abstract: This paper identifies the key risks the U.S. government and private energy-related corporations face within the Energy Sector. Specifically, the author examines the current risk strategies and controls within the Energy Sector, and then concludes with recommendations about how key stakeholders can improve resiliency.

Critical infrastructure has long been a major source of concern for the U.S. in wartime and in peace. Keeping our nation's financial, transportation, and energy systems up and running at all times is integral to economic and societal success. The landscape of risk associated with our critical infrastructure runs everywhere thanks to the growing interconnectivity of systems in the modern age. For example, without our Communications infrastructure running smoothly, our Finance and Transportation sectors would be unable to function effectively and likely collapse. While all sixteen of the infrastructure sectors our Department of Homeland Security (DHS) defines as "critical" are key to this country's stability, there is one in particular that acts as the bedrock of them all – the Energy sector.[1]

The DHS divides the Energy sector into three interrelated categories: electricity, oil, and natural gas.[2] The U.S. has more than 6,413 power plants spread across the country being powered by combustible coal, nuclear power, and natural gas.[3] Due to the integrated nature of the Energy sector, the DHS has labeled it "uniquely critical because it provides an 'enabling function' across all critical infrastructure sectors."[4] Despite the fact that 80 percent of the country's energy infrastructure is owned by the private sector, it remains a major source of concern for our government.[5] Any malfunction or attack on this infrastructure has the potential to shut down our country abruptly and make even the simplest day-to-day tasks impossible for citizens. This paper will look to identify the key risks our government and private energy-related corporations face moving forward, their current risk strategies and controls, and concludes with recommendations about how key stakeholders can improve resiliency.

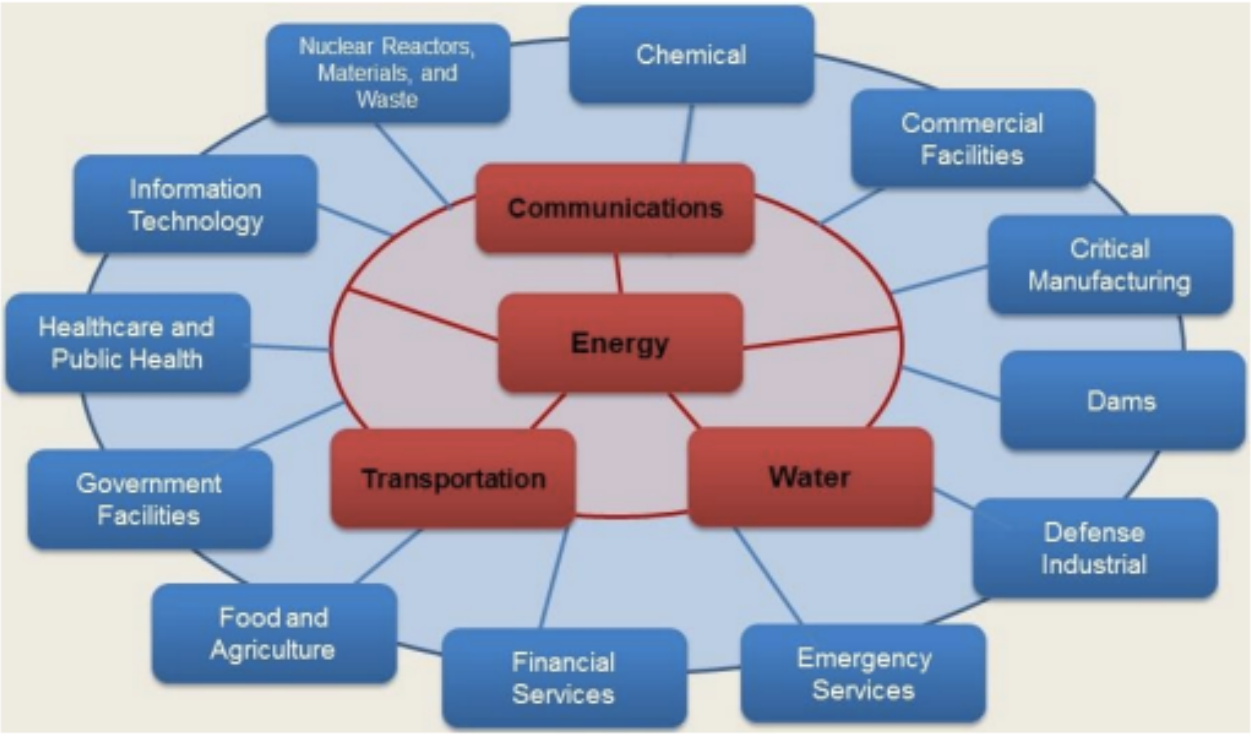
On the federal government side, the U.S. Department of Energy (DOE) oversees the Energy sector and is responsible for general risk management duties. In the 2015 annual report written in conjunction with the Department of Homeland Security (DHS), the DOE lays out a number of key tasks for the agency moving forward. These tasks include:

> "Strengthening the resilience of supply chains, enhancing cyber and physical security, examining interdependencies within the Energy Sector and across other sectors, enhancing climate resilience, addressing the risk associated with aging infrastructure and workforce, and developing meaningful metrics to assess the sector's progress toward security and resilience."[6]

All it takes is a quick scan of this list to see that risk mitigation is the main priority for the DOE. Clearly, the DOE recognizes the importance of the energy sector (and related infrastructure) and

is focusing its attention on risk prevention and the mitigation of negative risk events. The two risks the paper will focus on from the government perspective are 1) the interdependencies within the energy sector and 2) the reliance on private sector partners to help keep critical infrastructure up and running.

The Energy sector is incredibly complicated and diverse thanks to critical infrastructure that spans city, county, and state boundaries. The DOE must fully understand and map out all of these interdependencies in order to properly protect and control critical assets. Their annual report discusses the technology advancements of the 20th century as a catalyst for reliance on interdependencies between systems and stakeholders.[7] The energy-sector infrastructure in the U.S. is tied into the communication, information technology, transportation, and even financial service infrastructures. The following table from the DOE report gives a visual example of these infrastructure interdependencies:



Source: U.S. Department of Energy 2015 Energy-Specific Report[8]

This becomes important in the event of a disruption of one form or another. The connectivity of the system means that any disruption has the potential to cause wide spread effects on our country.

Hypothetical Scenario

Let us walk through a hypothetical scenario in which a simple attack on a power grid in California could have devastating effects on the biggest financial firms located across the country in New York City. Imagine a malicious hacker, be it a cyberterrorist or just a common "computer nerd" trying out a new method, gets into California's electrical grid control system and shuts down power to the Los Angeles basin. The resulting blackout could possibly decommission the communication networks that connect the Los Angeles-based financial institutions to their

colleagues in New York City. Critical cross-country networks could be affected and investment management firms attempting to complete trades on the New York Stock Exchange would be unable to get orders filled. This could potentially result in millions of dollars of losses depending on how financial markets reacted to the news of a major blackout in the country's second largest city. Information technology companies based in Silicon Valley could also feel the effects of sweeping blackouts if they were not prepared with backup servers in locations far enough away to not be effected. Business could come to a halt resulting in loss of revenues and plunging stock prices.

While this may seem like a scene from a movie, it is not entirely out of the realm of possibility. Earlier this year, Ukraine's power grid was completely shut down by hackers. The country was without power for an extended period before engineers could restart the system manually at substations.[9] Closer to home, a study by the Federal Energy Commission (FEC) noted that an attack on just nine critical substations scattered across the country would likely cause a national power outage that would last weeks or months.[10] The ever-increasing interconnectivity of our critical infrastructure will make events like this more common going forward and the DOE must put a special emphasis on preparing for risk events that can potentially permeate to other critical infrastructure sectors.

Accomplishing this goal will require the cooperation of the private sector – a majority owner of the physical energy infrastructure in this country. Managing the private sector and the way private corporations operate and secure their physical energy infrastructure presents a

second formidable risk to the DOE. As private corporations must deal with third-party risk from vendors and suppliers, the U.S. federal government must effectively manage third-party risk associated with the owners of our critical energy infrastructure. PwC, a consulting firm, recommends applying a stratification process to third-party risk management in which firms identify third parties that carry the most potential risk and then prioritize accordingly.[11] Though this recommendation is meant for the private sector, it would translate nicely to the DOE's oversight of private corporations under their mandate as well as their general risk management process. Ultimately, private corporations have a much narrower view of the risks associated with their infrastructure and it is up to the U.S. government and the DOE to provide oversight and monitoring in order to protect our country on a wider scale.

Private Sector Risks

As private corporations make up 80 percent of the ownership of energy infrastructure in this country, it is important to touch on the risks associated with these businesses. This paper will focus on two companies, FirstEnergy and Florida Power and Light; both of which have firsthand experience with the large-scale ramifications of improper risk controls.

FirstEnergy is an Akron, Ohio-based diversified energy company, and touts itself as one of the largest investor-owned electric systems in the country. They operate more than 240,000 transmission lines in the Midwest and Mid-Atlantic regions.[12] In 2003, poor weather led to falling trees and sagging power lines that eventually found themselves tangled up. Almost immediately, customers began calling FirstEnergy to let them know they had weak power and tripping

transmission lines. At the time, FirstEnergy did have an emergency alert system in place, but due to a system error, FirstEnergy controllers failed to notice any of the issues. They disregarded the customer complaints and assumed the poor electricity distribution was a competitor's fault. Not long after the complaints began, the FirstEnergy control room went dark, and the system controllers realized they had a major issue.[13] It was eventually determined that the malfunction in FirstEnergy's control systems was due to a bug in their computer code. Spokesperson Ralph DiNicola said at the time that the "fault was so deeply embedded, it took [developers] weeks of poring through millions of lines of code and data to find it."[14] The cascading effect of the blackout that could not be controlled (in large part due to the lack of early awareness from FirstEnergy) led to 50 million people in eight states and Canada being left without electricity.[15]

The example of FirstEnergy points to the importance of controlling system risks in the Energy sector. As much (if not all) of the critical infrastructure in the sector is controlled by computers, there must be a tight risk management controls in place to assure 99.9999 percent uptime of all systems. There should also be backup systems in place that, at the very least, can help prevent blackouts from spreading through the electrical system. Making a mistake in one line out of millions of code is one thing; not having a workaround that allows you to prevent further damage is another.

In fairness to FirstEnergy, they do acknowledge the risk involved in operating complex systems in their 10K reports. They mention the risk surrounding their infrastructure due to aging equipment and weather related events. They also refer to the interconnected nature of the

business and how this potentially poses risks to system functionality.[16] It seems safe to assume that the 2003 incident was a wake up call for the company, and subsequently their risk management (including the acknowledgement of potential risk) has improved over the last decade.

Our second victim of poor risk management in the private energy sector is Florida Power and Light (FP&L). Much like FirstEnergy, FP&L is a large electricity provider responsible for nearly 4.8 million customers in Florida.[17] The company has a very good track record of providing excellent service to customers and has been ranked in the top ten of Fortune's "World's Most Admired Companies" list.[18] With such an impressive resume, it would be easy to assume that FP&L's risk management function has performed flawlessly. As the following example will show, however, even the smallest oversight by a single employee can lead to widespread outages in the energy sector. It will also prove the importance of forcing employees to adhere strictly to the processes put in place in order to mitigate risk.

In February of 2008, a FP&L engineer was investigating a malfunctioning switch at one of the company's electricity substations in West Miami. In order to diagnose the issue with the switch, he disabled two levels of relay protection – a practice that was frowned upon by his employer.[19] Protective relays are "safety devices that monitor changes in the grid and are responsible for tripping breakers if conditions enter a danger zone that could harm transmission lines."[20] In disabling the relay protection, he opened up the possibility of any potential issue at that particular substation to radiate out and effect a large portion of the grid. Unfortunately for

the engineer and FP&L, a fault happened to occur while the relay protection was disabled and caused an outage affecting 26 transmission lines and 38 substations. In all, 584,000 customers were left without power.[21] Immediately after the incident, FP&L President Armando Olivera was forced to issue an apology and assured the public that they were implementing "interim changes governing relay protections to prevent a recurrence."[22]

This incident is a prime example of how the threat of "people risk" constantly hovers over a business. Despite having a strict policy in place that prevents both levels of protection from being disabled, the engineer went ahead anyway and removed the protections. Whether it was negligence or lack of procedural knowledge that prompted the engineer to disable the protections, the point remains the same – private corporations are constantly at risk of losing customers, money, and reputation due to the follies of individual employees. In this particular instance, FP&L could have prevented this issue with two very simple steps: 1) better oversight of their employees in the field and 2) better training on how and when engineers are allowed to disable mission critical safety devices.

Recommendations

So far, this paper has discussed a number of specific risk management recommendations for each of the energy related entities discussed thus far. This section presents two general recommendations for the sector as a whole. The first recommendation would be for greater segmentation of the U.S. energy infrastructure. As the system currently stands, it is far too easy for internal or external events to bring large portions of our energy infrastructure to its knees.

Much like the President and Vice President never fly on the same plane, the energy sector's infrastructure should be kept segmented in the off chance that a dramatic risk event does take place and a need arises for alternate electricity to get the country up and running again. Corporations who rely on electricity to power mission critical technology would feel safer knowing that if one electric grid goes down, it would not affect their backup technologies in different locations. Admittedly, more segmentation may create certain inefficiencies in the system and lead to extra costs. However, these extra financial costs are unlikely to match the monetary and social costs of an event that shuts down our county's entire electrical grid.

The second recommendation would be the improvement and evolution of cybersecurity defenses in the sector. While this is certainly not a novel idea and is already a major focus for the DOE, the importance of preventing cyber attacks on our energy infrastructure cannot be overstated. It is common knowledge that cyber warfare is fast overtaking physical warfare across the globe. As the U.S. energy infrastructure continues to become increasingly computer driven, it will also become a more prominent target for foreign countries with a vendetta. Critical infrastructure in the U.S> has historically been safe thanks to the geographical distance between the country and its enemies. Cyber warfare greatly reduces that advantage.[23] Thanks to the release of information about events like Stuxnet, the computer virus that helped slow down the Iranian nuclear program, it is known that these types of attacks are already occurring. The DOE must find a way to incentivize the brightest cybersecurity minds to come work for them and the private companies the DOE watches over. If that means hiring brilliantly skilled individuals with

coding and hacking abilities who typically would not fit into a corporate or government environment (think high school drop-outs), so be it.

Conclusion

It must be understood that the risks associated with the country's energy sector are far too great to go unnoticed. Electrical grids, gas, and nuclear power provide the backbone for the U.S. and allow its other critical infrastructure to operate successfully. The DOE has an incredibly important role in overseeing and closely monitoring the private companies that operate underneath them. Without an evolving risk management strategy, the DOE runs the risk of allowing major security holes to open up in an increasingly hostile world. The U.S. government already has a policy of using "all means necessary" to respond to a digital attack on a U.S. operated electrical grid (including physical retaliation), but prevention and risk mitigation should clearly be favored over hostile retaliatory actions.[24] By mandating better segmentation of systems and bulking up cybersecurity defenses, the DOE would be announcing to the world that the U.S. takes security of its critical infrastructure very seriously and may just focus the spotlight on the sector long enough to attract the next generation of great minds to solve the country's most important problems.

Works Cited

[1] Department of Homeland Security. (27 Oct. 2015). "Critical Infrastructure Sectors." Retrieved 15 Feb. 2016 from <http://www.dhs.gov/critical-infrastructure-sectors>
[2] Department of Homeland Security. (19 Jan. 2016). "Energy Sector." Retrieved 15 Feb. 2016 from <http://www.dhs.gov/energy-sector#>
[3] Ibid
[4] Ibid

[5] Ibid

[6] Department of Homeland Security. (2015) "Energy Sector-Specific Plan." Retrieved 15 Feb. 2016 from <http://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf>

[7] Ibid

[8] Ibid

[9] Kuchler, H. & Buckley, N. (5 Jan. 2016). "Hackers Shut Down Ukraine Power Grid." Retrieved 20 Feb. 2016 from <http://www.ft.com/intl/cms/s/0/0cfffe1e-b3cd-11e5-8358-9a82b43f6b2f.html#axzz40eqLeOj4>

[10] Smith, R. (12 Mar. 2014). "U.S. Risks National Blackout from Small-Scale Attack." Retrieved 20 Feb. 2016 from <http://www.wsj.com/articles/SB10001424052702304020104579433670284061220>

[11] PricewaterhouseCoopers. (Nov. 2013). "Significant Others: How Companies can Manage the Risks of Vendor Relationships." Retrieved 22 Feb. 2016 from <https://www.pwc.com/us/en/risk-assurance-services/assets/pwc-viewpoint-vendor-risk-management.pdf>

[12] FirstEnergy. (12 Feb. 2016). "About Us." Retrieved 20 Feb. 2016 from <https://www.firstenergycorp.com/about.html>

[13] Zetter, K. (2014). *Countdown to Zero Day*. New York, NY: Broadway Books. Pg. 159

[14] Poulsen, K. (11 Feb. 2004). "Software Bug Contributed to Blackout." Retrieved 22 Feb. 2016 from <http://www.securityfocus.com/news/8016>

[15] Ibid

[16] FirstEnergy. (2015). "FirstEnergy 2015 10K." Retrieved 22 Feb. 2016 from <https://www.firstenergycorp.com/content/dam/investor/files/10-K/2014-10K.pdf>

[17] Florida Power and Light. (2016). "Company Profile." Retrieved 23 Feb. 2016 from <https://www.fpl.com/about/company-profile.html>

[18] Ibid

[19] Florida Power and Light Newsroom. (29 Feb. 2008). "FPL Announces Preliminary Findings of Outage Investigation." Retrieved 23 Feb. 2016 from <http://newsroom.fpl.com/news-releases?item=101775>

[20] Zetter, K. (2014). *Countdown to Zero Day*. New York, NY: Broadway Books. Pg. 161

[21] Florida Power and Light Newsroom. (29 Feb. 2008). "FPL Announces Preliminary Findings of Outage Investigation." Retrieved 23 Feb. 2016 from <http://newsroom.fpl.com/news-releases?item=101775>

[22] Ibid

[23] Zetter, K. (2014). *Countdown to Zero Day*. New York, NY: Broadway Books. Pg. 377

[24] Ibid. Pg. 398