Proceedings of 2022 Asian Conference on Crisisonomy
(20 ~ 23 July, 2022; Jeju National University; Asian Association for Crisisonomy)

Protecting the Texas Electric Grid

Jennifer Holmes

School of Economic, Political and Policy Sciences University of Texas at Dallas (GR 31) 800 W Campbell Road Richardson

1. INTRODUCTION AND RESEARCH MOTIVATION

Two recent events have alerted American policymakers at all levels of government to refocus their efforts on grid security. First, the December 2015 and 2016 successful cyberattacks on Ukraine's electric infrastructure represented a "wake-up-call" for policymakers, industry insiders, and the population at large (Mission Support Center 2016, Trabish 2017). Another warning came in the summer 2017 during an attempted cyberattack on a petrochemical plant in Saudi Arabia. This attack, although foiled due to an error in the code, could have led to a complete takeover of the plant by the attackers, including the possibility of the release of toxic gases (Giles, 2019). However, preventing cyberattacks is expensive, and while the events themselves are rare, they are extremely disruptive to the economy. A 2015 Lloyd's white paper (Lloyd's, 2015) suggests that an 'Erebos' malware attack on the eastern US grid could have a $243 billion impact; even if some power was restored within 24 hours, many places would be without power for several weeks.

2. POLICY OPTIONS

What policy options exist to protect the Texas power grid? Texas has a unique regulatory structure which includes the Public Utility Commission of Texas (PUCT) and the Electric Reliability Council of Texas (ERCOT). Additionally, ERCOT must abide by NERC Critical Infrastructure Protection (CIP) standards. Electricity generation, transmission, distribution, and delivery in the United States is regulated at federal, state, and local levels of government. Both FERC, as the government "side", and NERC, as the industry "side", work to oversee the regional transmission organizations (RTOs) as they work to ensure reliability on the issue of cybersecurity. Therefore, while there may be differences between the RTOs, they all are supposed to abide by the CIP standards.

3. ISSUES WITH NERC CIP COMPLIANCE

CIP standards force compliance, but not necessarily enhanced security or reliability (Miller interview, 2017). There is a disconnect between the goal of energy policies and regulations and how they are being implemented by the industry. In 2009, a self-certification survey performed by NERC found that less than one-third of generation owners believed they had a critical asset which required following CIP standards (Hegrat and Case, 2010). Additionally, not all utilities are subject to CIP standards. Any utility that generates or transmits less than 300 MW of electricity is exempt from the requirements. This is about 84% of all Texas utility companies. This vulnerability and compliance loophole with cybersecurity standards should be addressed and closed. Some utilities are better equipped to handle the additional requirements while others are not. In general, industry tries to minimize costs while also ensuring a well-defended system that complies with all applicable laws. A 2013 Brookings Institute argues for federal offering tax incentives and subsidies to create compliance.

4. STATE APPROACHES TO CYBERSECURITY IN THE POWER GRID

Since cyberattacks are such high impact, low probability events, the federal and state governments have a difficult time in knowing the best methods to detect and defeat them and often do not prepare for them (Flynn 2007) . Cohen and Nussbaum (2018) studied three different approaches to cybersecurity in Arizona, New Jersey, and Washington and compared them to gather insights into best practices. Arizona's "community approach" leverages relevant public-private partnerships to keep each other abreast of any cybersecurity issues or development opportunities. New Jersey's "bureaucratic superstructure" used the public sector as a centralized organizer from which decisions are handed down to utility companies. Lastly, the Washington "multidisciplinary" approach melds the public sector organizational structure of the New Jersey model with the private-public trust model of Arizona to create, in their view, a mature model of how cybersecurity issues ought to be handled. The Texas approach is more akin to the Arizona model than the other two, but it is possible that given ERCOT's independence, the centralizing aspect of cyber coordination as found in the Washington model is still possible; however, those functions would be carried out by ERCOT and not the state of Texas.

5. HOW TEXAS CAN LEAD THE WAY

A. ERCOT

ERCOT is the only Independent System Operator (ISO) that is not directly regulated by the federal government. As the sole RTO for the Texas Interconnection, it is independent of all the other grids and interconnections, with only two ties to the Eastern Interconnection and one to the Western Interconnection. While states have authority to regulate the distribution and sale of power within their borders, the independence of the ERCOT connection means that the Texas legislature has more prerogative than other states in regulating the generation and transmission of power. This is done through the PUCT, which is responsible for both the generation/transmission and the consumption side for the entire state, not just ERCOT. Texas is uniquely placed among the states as a laboratory to experiment and improve the standards at the supply and demand levels.

6. POTENTIAL SOLUTIONS

A key insight into the fundamental weakness of the current approach is that the successful attacks witnessed to date have been on the distribution systems, and not the generation systems (Mission Control Center 2016). CIP standards focus on protecting generation and transmission assets. However, a cyber-attacker may still cause significant damages by targeting distribution utilities.

Two tactics can strengthen the grid: a centralization of communication at the state regulatory level, and increased flexibility to effectively deal with problems at the individual utility level. Texas could adopt the Washington model to create a bureaucratic hierarchy within the regulatory agencies to centralize command and communication operations. This way, the state agency could be quickly notified of any problems at the individual level. The existing Texas "public-private" partnerships could be augmented with ERCOT and the PUCT providing best practices and a clearinghouse for communications.

Second, three things could be done to harden the electricity infrastructure in Texas: 1) Establish a grant program for CIP compliance specifically aimed at municipalities and cooperatives. Grants can be used to enforce standards; continued funding could be conditional upon meeting the guidelines ERCOT sets. This funding mechanism could give utilities the "nudge" they need to incorporate CIP standards over their objections. 2) Streamline the auditing process to set one "high water mark" for meeting standards. There are different standards assigned to different pieces of equipment. If most, if not all, equipment is held to the same CIP standard, then utilities would be able to easier handle compliance, and, perhaps more importantly, regulators could become more efficient at performing audits and spot checks. 3) promote the role of grid insurance companies. Insurance companies provide a market-based solution to the negative externalities cyberattacks. If insurance companies began to demand CIP compliance as a precondition for coverage, utilities may respond favorably.

Disaster insurance is a common approach for businesses to mitigate risks of events they cannot control. However, typically insurers will not enter a market unless they can appropriately price the risk. We propose a public-private partnership whereby ERCOT and/or the PUCT "war-game" the possibilities of what different types of cyberattacks on various utility generation and transmission companies would do to the companies' infrastructure. This data could in turn be shared with insurance and reinsurance companies so they could model and therefore price the risk. A current area where this type of collaborative approach is working is in the pricing of climate change insurance. The state of Washington is working with insurance companies to model and price the expected effects of natural disasters strengthened by climate change (Washington Office of the Insurance Commissioner).

7. CONCLUSION

As global technological interconnectedness proliferates, policymakers face increasing cyber threats against their critical infrastructure systems. The decentralized nature of the US grid makes coordinated responses to such an attack more difficult; however, it also reduces the likelihood of a catastrophic event. The state of Texas, along with the Public Utility Commission and ERCOT, has an opportunity to lead the way forward in grid preparedness due to its relative independence from federal regulations.

Through leveraging its regulatory independence, Texas can experiment with stronger security protocols, as well as policy reforms, to make cybersecurity adoption more robust across the electric grid. Specifically, the Texas legislature can create a grant fund, to be assigned through ERCOT and/or the PUCT, for municipalities and cooperatives who may be more hesitant to adopt the reforms. Also, ERCOT and the PUCT can take the existing NERC CIP standards and remove their more confusing aspects, thereby streamlining the compliance aspect. Finally, they can ensure that utilities still unwilling to adopt standards can implement more robust procedures for a quick transition away from a digital operating process to a manual one in the case of an attack, thereby removing the affected utility from the remainder of the grid.

Acknowledgement: This work was supported in part by NSF CRISP awards CMMI-1925524 and CMMI-1541159, and by the Texas National Security Network.

References

Bialek, J. W. (2010). Critical interrelations between ICT and electricity systems. In Z. Lukszo, G. Deconinck, and M. P. C. Weijnen (Eds.), Securing electricity supply in the cyber age: Exploring the risks of information and communications technology in tomorrow's electricity infrastructure, Chapter 4, pp. 53–70. London: Springer.

Brady, M. (2006). 1906 San Francisco earthquake shook up the insurance industry worldwide. National Underwriter Property & Casualty.

Cohen, N. and B. Nussbaum (2018). Cybersecurity for the states: lessons from across America. New America Working Paper.

Fitzgerald, Trey. Cybersecurity, NERC and Solar O&M in Texas. Presentation sponsored by Husch Blackwell; 17 May 2019 accessed at https://www.huschblackwell.com/newsandinsights/cybersecurity-nerc-and-solar-om-in-texas

Fleisher, Jared M. (2008). ERCOT's Jurisdictional Status: A Legal History and Contemporary Appraisal. Texas Journal of Oil, Gas, and Energy Law 3(1), 5-21.

Flynn, Stephen. (2007) Edge of Disaster. Random House

Giles, M. (2019). Triton is the world's most murderous malware, and it's spreading. MIT Technology Review.

Hegrat, B. and C. Case (2010). Protecting critical infrastructure and cyber assets in power generation and distribution. Rockwell Automation.

Insua, David Rios, A. C.-V. and K. Musaraj (2018). Some risk analysis problems in cyber insurance economics. Estudios de Economia Aplicada 36(1), 181– 194.

Langham, R. and P. Pederson (2013). Bound to fail; why cyber security risk cannot simply be 'managed' away. Brookings Institution.

Lloyd's (2015). Business blackout: The insurance implications of a cyber-attack on the us power grid. Emerging Risk Report, Innovation Series.

Petersen, Dale (2017). Interview with Patrick Miller. Accessed at https://itunes.apple.com/us/podcast/unsolicited-response-podcast/id1240062226?mt=2&i=1000391947871

Malashenko, Elizaveta, Chris Villarreal, and J. David Erikson. "Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission." California Public Utilities Commission. September 19, 2012.

Masera, M. (2010). Governance: How to deal with ICT security in the power infrastructure? In Z. Lukszo, G. Deconinck, and M. P. C. Weijnen (Eds.), Securing electricity supply in the cyber age: Exploring the risks of information and communications technology in tomorrow's electricity infrastructure, Chapter 6, pp. 111–128. London: Springer.

Mission Support Center, Idaho National Laboratory (2016). Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector.

Neuhauser, Alan. "Cyberattacks surge on energy companies, electric grid." US New and World Report. April 6, 2016.

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: how insurance companies act as 'compliance managers' for businesses. Law & Social Inquiry 43(2), 417–440.

Trabish, Herman K. "Why utilities say grid security is the most pressing sector issue of 2017." Utility Dive. April 10, 2017. https://www.utilitydive.com/news/why-utilities-say-grid-security-is-the-most-pressing-sector-issue-of-2017/440056/.

US Department of Homeland Security (2018). US Department of Homeland Security Cybersecurity Strategy. Washington, DC.

Washington Office of the Insurance Commissioner. Accessed at https://www.insurance.wa.gov/insurance-commissioners-work-climate-risk-and-insurance.

Wildman, Leonard D. (Capt.). Memorandum to the Military Secretary. The Museum of the City of San Francisco. Accessed at http://www.sfmuseum.org/1906.2/arson.html.