Securing Electric Grids

By: Gerald Rigdon - 2023

According to IBM's Threat Intelligence Index report (Gregory, J., 2023) nearly 11% of the cyberattacks that were handled by their Security X-Force during 2022 were in the energy sector. One example of a physical attack was the 2022 shooting of a power grid substation in North Carolina (Cama, T., 2022), which affected 34,000 customers during frigid temperatures. Another recent attack against an undisclosed Asian country (Greenberg, A., 2023) from a threat group linked to Chinese-origin cyber spies or APT41 began in February 2023 and lasted six months. Closer to home (Koski, R., 2023) reported on an investigation underway for malware in computer systems that control utilities, and the Texas power grid was a concern given three major military installations exist there. So, assuming Austin Texas was the target of an electric grid cyber-attack, how could one anticipate the societal consequences?

In terms of social impact of power outages, one of the most extensive research papers (Andresen, A., Kurtz, L., Hondula, D., Meerow, S., Gall, M., 2023) was recently published and highlighted the following:

- The 2021 American Society for Civil Engineers infrastructure report rated the U.S. power grid as mediocre.
- The power grid system is highly interdependent with other critical infrastructure such as water and communication networks.
- Most affected groups are children, older adults, racial and ethnic minorities, and those in rural areas.
- Criminal acts increase during outages and looting occurs in areas with lower socio-economic advantage.
- CO poisoning occurrences increase due to unsafe generator use.
- People dependent on medical equipment and devices are more vulnerable.
- Food illnesses increase due to consumption of spoiled food.
- The research is limited and more needs to be done.

Unfortunately, while (Andresen, A., Kurtz, L., Hondula, D., Meerow, S., Gall, M., 2023) offered a lot in terms of impact and risk, not much was said about mitigation and risk management. In (*5 Strategies for Reducing the Harmful Consequences from Loss of Grid Power*, 2017), the following recommendations involving key government agencies such as the Department of Energy, the Department of Homeland Security, and State Authorities would be effective as part of an overall risk management plan:

1. Oversee regular and systematic testing of backup power generation equipment at critical facilities.
2. Develop guidance and investments in advanced control technologies to supply particular feeders for critical users to mitigate the impact of long-duration and large area outages.
3. Develop guidance on selective restoration, factors involved in which loads to serve, and how to adapt to local circumstances.
4. Determine the best approach for getting critical facility managers to pre-register information about emergency power needs.
5. Help regional and local planners envision the effects of long-duration power loss.

In terms of practical measures to mitigate the aforementioned societal and social impact, the final recommendation above (*5 Strategies*, 2017) of helping local planners envision the effects of long-duration power loss could be a modelling exercise which would assist in quantifying the total number of people involved in certain geographies and ultimately how many of those represent the most vulnerable groups. These efforts involving predictive analytics are important approaches to security and resiliency.

As for roles and responsibilities, per (*Public Power Cyber Incident Response Playbook*, 2019) this should be a collective, group effort involving not only utility staff but also other municipal employees, and third-party resources including federal, state, and city agencies. In Step1 of the *Playbook*, every electric utility company should establish a Cyber Incident Response Team or CIRT that is further decomposed into a First Response Team, a CIRT Steering Committee, and finally a Full CIRT or a complete list of people with assigned roles that can be called upon as needed to scale-up and support a response to power grid cyber-attacks.

References:

5 Strategies for Reducing the Harmful Consequences from Loss of Grid Power (2017). nap.nationalacadamies.org. https://nap.nationalacademies.org/read/24836/chapter/7#106

Andresen, A., Kurtz, L., Hondula, D., Meerow, S., Gall, M. (2023, May). *Understanding the social impacts of power outages in North America: a systematic review.* iopscience.ioo.org. https://iopscience.iop.org/article/10.1088/1748-9326/acc7b9

Cama, T. (2022, December). *Who shot the North Carolina power grid?* politico.com. https://www.politico.com/newsletters/power-switch/2022/12/05/who-shot-the-north-carolina-power-grid-00072235

Greenberg, A. (2023, September). *China-Linked Hackers Breached a Power Grid-Again.* wired.com. https://www.wired.com/story/china-redfly-power-grid-cyberattack-asia/

Gregory, J. (2023, May). *Today's biggest threats against the energy grid Today's biggest threats against the energy grid.* securityintelligence.com. https://securityintelligence.com/articles/todays-biggest-threats-against-the-energy-grid/

Koski, R. (2023, July). *Malware from China could target Texas power grid, utilities.* fox7.austin.com. https://www.fox7austin.com/news/texas-power-grid-utilities-possible-malware-target

Public Power Cyber Incident Response Playbook (2019, August). publicpower.org. https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.