GLOBAL CYBER POLICY WATCH

CRITICAL INFRASTRUCTURE AND CYBERSECURITY:
A CLOSER LOOK AT THE LIQUEFIED NATURAL GAS INDUSTRY

SEPTEMBER 2018

WWW.GLOBALCYBERPOLICYWATCH.COM

Critical Infrastructure and Cybersecurity:
A Closer Look at the Liquefied Natural Gas Industry

The cybersecurity of our national critical infrastructure is a top-tier national security concern. With increased reports of foreign actors targeting, meddling, and hacking America's energy infrastructure, it is worth examining what stakeholders are doing to protect themselves. The following issue brief examines how the natural gas industry is tackling today's rising cybersecurity risks.

Executive Summary

- **The LNG industry Is Committed to Federal Partnership.** In April of 2018, the National Institute of Standards and Technology (NIST) updated their official framework of cybersecurity objectives and standards. Energy producers worked alongside NST in developing this crucial guide, and LNG companies continue to implement the framework into their cybersecurity playbook.
- **Close Department of Energy Engagement.** Utilizing the DOE's Oil and Natural Gas Cybersecurity Capability Maturity Model, natural gas companies are participating in self evaluation methodology. This public/private partnership helps firms identify and improve their cybersecurity.
- **Information Sharing Within the LNG Sector.** More than 50 natural gas and oil companies have come together in the Oil and Natural Gas Information Sharing and Analysis Center (ONG ISAC). Allowing members to share threat information, this communication allows members identify threats and develop responses in coordination with each other and the federal government.
- **Ensuring Strong Cybersecurity Requires Training.** This year, representatives participated in the GridEx IV training exercises put on by the North American Electric Reliability Corporation (NERC). Joining government and gas industry leaders, these exercises allow firms to identify weakness and test their response capabilities during simulated cyber attacks on our power grid.
- **Developing and Investing In New and Secure Technologies.** In recent years, LNG companies have invested millions of dollars into sophisticated technologies to improve distributed control systems, cloud based services, and data analytics. By investing in critical cyber defense technology, firms are giving their workforce the capability to adapt to emerging cyber threats.
- **LNG Is Simply Safer Than Nuclear Energy.** LNG is able to quickly defuse different networks of pipelines, which impedes and limits the effects of a cyber attack. Alternatively, nuclear energy requires large amounts of nuclear material be stored on location. The inherent threat posed by nuclear energy to the environment and civilians seriously escalates the impact of a nuclear targeted cyberattack.
- **Nuclear Systems Are Vulnerable to Cyberattacks.** Despite nuclear executives claiming their systems are protected from cyberattacks through "air gaps," many nuclear facilities rely on old equipment that requires frequent software updating. These processes open the door to breach potential.

Background

The cybersecurity of our energy sector is of the utmost importance to the safety and wellbeing of our nation. Vulnerable systems could allow domestic and foreign hackers to use our reliance on energy against us. So much of our daily lives depend on reliable energy delivery, and any disruption in the process would cause untold damage in economic costs and could very well lead to loss of life. With the energy sector facing millions of cyber threats each day, this is clearly a very real danger faced by every aspect of America's energy sector.[1]

One of the fastest growing industries within the energy sector is the Liquid Natural Gas (LNG) industry. In the early 2000s, there was 100 million tons of LNG sold each year. That number was nearly tripled for 2017.[2] In 2017, natural gas accounted for 29% of American energy consumption and 31.8% of our energy production. In both cases, natural gas was both consumed and produced at a larger percentage than coal and nuclear power combined.[3] With such statistics, it is no surprise that the industry has had a tremendous impact on the economy. In 2016, the LNG industry was responsible for employing around 3 million Americans.[4]

Since the LNG industry recognizes its important place in our economy and the grave cyber threats it is facing, the sector has been proactive in developing strong cyber practices and ensuring that its systems are protected from malicious hackers. The general public, that relies heavily on the LNG industry for everyday energy needs, deserves to know the specifics of the cyber risks facing the LNG industry and what the industry is doing to mitigate them.

Federal Engagement

In order to ensure that its infrastructure is secure, members of the LNG industry have been actively working together, as well as with the public sector, to develop resources and practices to help them protect their systems.

One such example of this work has been conducted in partnership with the National Institute of Standards and Technology (NIST). The United States energy industry has been working closely with NIST on an official framework of cybersecurity objectives and standards. The "Framework for Improving Critical Infrastructure Cybersecurity" was first published in 2014 after the passage of the Cybersecurity Enhancement Act of 2014. The framework was designed to arm businesses vital to the nation's economy and security with tools and practices that they can use to secure their systems from hostile actors.[5] The framework is a living document and is updated periodically to account for changes in both technology and the threat environment. The most recent update came in April 2018 when NIST released version 1.1, which LNG companies are in the process of adopting. This update includes new information regarding authentication & identity, self assessments of cybersecurity risks, cybersecurity in the supply chain, and vulnerability disclosures.[6]

Representatives of the natural gas industry have also engaged with the federal government through the Department of Energy's (DOE) Oil and Natural Gas Cybersecurity Capability Maturity Model (ONG C2M2). Released in 2014, the ONG C2M2 was derived from a similar model developed for the electric sector. The model was designed to be used with a self evaluation methodology in order to help companies measure and improve their cybersecurity. ONG C2M2 includes the 10 model domains of: Risk Management; Asset, Change, and Configuration Management; Identity and Access Management; Threat and Vulnerability Management; Situational Awareness; Information Sharing and Communications; Event and Incident Response and Continuity of Operations; Supply Chain and External Dependencies Management; Workforce Management; and Cybersecurity Program Management. Within each of these domains, ONG C2M2 lists out a number of steps that firms can take to improve their posture within that domain.[7]

---

https://www.bna.com/utilities_prepare_increased_n73014481471/

2 https://www.cnbc.com/2018/02/26/shell_warns_of_lng_shortage_as_demand_for_liquefied_natural_gas_booms.html

3 https://www.eia.gov/energyexplained/?page_us_energy_home

4 https://www.aga.org/sites/default/files/natural_gas_facts_final.pdf

5 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

6 https://www.nist.gov/news_events/news/2018/04/nist_releases_version_11_its_popular_cybersecurity_framework

7 https://le.utah.gov/interim/2017/pdf/00002604.pdf

Intra-Industry Cooperation

The development of the cyber frameworks outlined above have the added benefit of encouraging greater information sharing within the LNG sector. Because the security of our energy systems is of vital importance to our economy and national security, more than 50 natural gas and oil companies have come together in the Oil and Natural Gas Information Sharing and Analysis Center (ONG ISAC). Created in 2014, the ONG ISAC serves as a tool for its members to share threat information with each other and with the federal government. This form of communication allows members to be prepared for threats and to develop a coordinated response.[8] The ONG ISAC is modeled in the manner of other information centers, such as the Multi State Information Sharing and Analysis Center (MS ISAC), which currently shares information for thousands of American state, local, tribal, and territorial government units, and is touted by the Department of Homeland Security as one of the premier ISACs. Information sharing centers such as these are extremely valuable tools as they encourage greater cooperation among competing firms in order to develop stronger resilience among the industry as a whole.[9]

The NIST framework and the ONG ISAC serve as incredibly useful resources for the LNG industry. Yet having the right tools and resources is insufficient to ensure strong cyber capabilities. Organizations must also have the ability to implement these practices effectively. Therefore, the LNG industry is actively working to hone these skills. This past year, representatives from the gas industry took part in the GridEx IV training exercises put on by the North American Electric Reliability Corporation (NERC). GridEx is a biennial, two day exercise that brings together industry and government leaders to address their response capabilities to simulated attacks on our power grid. These types of exercises allow firms to test their abilities to respond to a cyber threat, giving them the chance to identify where their weaknesses lie and how they can be better prepared moving forward.

Common Practices

In addition to the industry developing processes and frameworks for addressing cyber threats, there are several cyber practices that are common among the many members of the LNG industry. One of the most important steps that LNG companies have taken is the development of new, more secure technologies. For example, in 2016 ExxonMobil launched the Open Process Automation Forum (OPAF), an initiative dedicated to defining an interoperable control architecture. OPAF has since become a forum of The Open Group. Among its other goals, OPAF is being used as opportunity to develop distributed control systems (DCS) that are better able to adapt to future cloud based services.[10] ExxonMobil contracted Lockheed Martin with the development and integration of these new DCS. At the announcement of their partnership in 2015, the two firms said that the new technology will have the capability to adapt to emerging cyber threats.[11]

Many LNG firms have also begun to use the power of data analytics to improve the security of their systems. Chevron, for example, has implemented a technology qualification process (TQP) in both its information technology (IT) and operational technology (OT) departments.[12] Originally used in the company's oil engineering side, Chevron's TQP uses a 9 point scale to describe a technology's level of maturity, reflecting the uncertainty of its technological readiness. The process uses data science to quantify the level of risk associated with different technologies and to label them using non technical language that is consistent across sectors within the company. Although traditionally TQPs are used after a capital commitment has been made to use the technology, Chevron is using them to screen and select the best technologies before their deployment.[13]

In order to implement the measures outlined above, firms have had to invest millions of dollars into their cyber capabilities. In order to continue improving their ability to detect and to respond to cyber attacks, LNG firms have committed themselves to continue to make these investments and test the readiness

8 http://ongisac.org/
9 https://securityintelligence.com/how_can_an_isac_improve_cybersecurity_and_resilience/
0 https://www.isa.org/intech/20180201/
https://www.controlglobal.com/industrynews/2016/exxonmobil_picks_lockheed_martin_to_develop_open_secure_dcs/
2 https://www.itnews.com.au/news/chevron_injects_data_science_into_infosec_operations_451311
3 https://www.researchgate.net/publication/266671817_Using_Technology_Classification_and_Qualification_Status_as_a_Tool_for_Strategic_Technology_Screening_and_Selection

of their cyber systems and workforce. One such commitment has come from Dominion Energy who is currently planning to invest an additional $50 million in its cybersecurity defenses through 2022. Further, Dominion recently committed itself to conducting numerous exercises to address cyber vulnerabilities, including several penetration tests and independent vulnerability scans.[14] By investing in their cyber defenses and their workforce, firms are staying on the top of the ever changing threat environment. The LNG industry understands that as hackers continue to develop new ways to infiltrate systems, they too will need to evolve and develop new and more sophisticated defenses.

LNG Advantage

In addition to the numerous measures the LNG industry has taken to protect itself from cyber threats, the nature of LNG gives it a cyber advantage over other forms of energy. One of the biggest advantages of LNG is its diffuse network of pipelines, which would impede the effects of a cyberattack. Comparatively, other energy producers, like nuclear energy, would have a weaker cyber posture due to the massive impact a cyberattack would have not just on the energy producer, but the environment and community around a nuclear plant. Nuclear energy companies tend to store massive amounts of nuclear material in a singular location. This fact, along with the dangers inherent to nuclear material, seriously raises the stakes of a cyberattack against a nuclear facility. One only needs to look at disasters at plants in Fukushima, Japan and Three Mile Island in the United States to understand the devastation that can occur if safety systems fail at a nuclear plant. Further, the Nuclear Regulatory Commission does not require plants to report attacks on their IT systems. This is an issue because the IT systems tend to be less protected than other systems.[15]

Both the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have disclosed information about attacks on the computer networks of companies operating nuclear facilities in the United States.[16] While the attacks thus far have not affected the operating systems of these facilities, some cybersecurity experts have suggested that the attacks were meant to gather intelligence and lay the groundwork for future attacks.[17] Representatives from the nuclear industry claim that their systems are impervious to cyberattacks because they are "air gapped", yet experts have emphasized that viruses could still infiltrate these systems through other vectors.[18] For example, because many nuclear facilities rely on old equipment with long expectancies, they need to frequently update these systems with new software and firmware. This update process could allow malware to bypass the air gap and to breach the systems.[19] And if an attack was successful, a nuclear plant could not be shutdown as readily as an LNG plant. Even after the reactor is turned off, the nuclear material will continue to decay and the core could still melt.[20] Such a meltdown would be devastating to the country and could leave a swath of the United State unlivable for generations.

Conclusion

One of the greatest challenges facing the energy sector is the growing threat of cyberattacks. As hostile actors continue to develop new tools and strategies to infiltrate unprepared systems, it is vital that companies are able to respond both quickly and effectively. The liquid natural gas industry has been proactive in strengthening its cyber defenses. Through intra industry cooperation and public sector engagement, LNG companies have effective at developing best practices to ensure that they can protect their systems, and thus our way of life.

---

4 https://sustainability.dominionenergy.com/downloads/DOM17CSR_Business_Future.pdf
5 https://www.theverge.com/2018/1/23/16920062/hacking_nuclear_systems_cyberattack
6 https://www.nytimes.com/2017/07/06/technology/nuclear_plant_hack_report.html
7 https://www.businessinsider.com/us_accuses_russia_of_hacking_energy_sector_to_gather_intel_for_attacks_2018_3
8 https://www.theverge.com/2018/1/23/16920062/hacking_nuclear_systems_cyberattack
9 https://www.bv.com/insights/expert_perspectives/cyberattacks_nuclear_power_plants_highlight_vulnerabilities_risk; https://www.independent.co.uk/news/world/nuclear_power_plants_vulnerable_hacking_attack_cyber_nightmare_united_nations_a7479546.html
20 http://large.stanford.edu/courses/2017/ph241/bunner2/docs/SI_v10_I1_Kesler.pdf