Talia Berler
CSC 116
Professor Sarkar
12/7/22

Cyber Threats to Critical Infrastructure: An Analysis of the Cyber Resilience of National Energy Sources

Abstract – *As digitalization increases across the globe and technology becomes rapidly more essential to the function of society, the vulnerability of nations and smaller municipalities rises proportionally. The backbone of modern life is energy, whether from fossil fuels or clean and renewable sources. The devastating consequences of poorly protected energy sources has been experienced in the aftermath of the Colonial Pipeline attack and other incidents of malicious actors infiltrating industrial control systems in and out of the US. This analysis of the cyber resilience of the US draws on information from recent attacks on the nation's critical energy infrastructure, government responses and measures, and expert advice from across the private sector. Since 2021, a great deal of progress has been made in improving cybersecurity standards and expectations on a federal level. However, the lack of oversight of the private sector has created a deficit of properly secured critical energy resources. Using the gathered information, this report finds that the government and private sector have neglected basic security measures and must dedicate more resources towards network segmentation, monitoring and reinforcing access to industrial control systems, and confidential communication of threats to protect vital energy channels.*

1. Introduction

As defined by Obama in 2013, critical infrastructure includes industries that are "...so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters..."[1]. This important distinction was released in one of two related executive orders created in 2013 and 2014, to establish critical infrastructure cybersecurity[2]. Following the Colonial Pipeline attack in 2021, Biden released Executive Order 14028, including key reforms such as requiring communication of threats between IT

service providers and the government, implementing stronger cybersecurity of federal technology and establishing the collaborative Cyber Safety Review Board[3]. The Cybersecurity and Infrastructure Agency (CISA) under the umbrella of the Department of Homeland Security (DHS) heads these reform efforts, though there are many government agencies involved in instilling these changes[4].

Despite these coordinated efforts in the public sector, the private sector controls 87% of the critical infrastructure in the US and shoulders far more responsibility in its protection[5]. These private companies deal with cyberattacks to critical infrastructure directly, and though the aforementioned executive orders have created channels of communication to share information with the government, they are complicated and underused[6]. Additionally, the federal orders do not mandate changes to private sector operations; the government hopes to "lead by example" with their reforms[7]. Therefore, private energy providers must take action to fortify their cybersecurity and resilience, and should draw upon shortcomings in previous attacks.

2. Cyber threats to the energy sector

The energy sector is integral to the functioning of modern society; systems of mass transit, essential lines of communication, healthcare systems, and defense technology all rely on national energy infrastructure[8]. Most of the country's energy comes from oil and gas pipelines[9] which are shifting towards automation and remote access control, and consequently, dependence on technology systems to function[10]. Furthermore, the global shift towards clean fuel sources, such as wind turbines and solar panels, creates more power sources connected straight to the grid[11]. Though heightened reliance on low polluting energy sources is vital to the future of the planet, it opens up national infrastructures to new and dangerous threats in cyberspace. All sources of energy, both new and old, are susceptible to attack through cyberspace.

Since energy is essential to societal function, providers are more likely to be targeted by malicious actors for a few reasons. First and foremost, the energy sector has a great deal of financial assets, being huge players in the US and global economy. The most frequent method of attack used on critical infrastructure in 2021 was ransomware[12]. Malicious actors know that these companies can make massive ransom payments if targeted by ransomware. Furthermore, halting operations of energy sources is highly disruptive, creating incentives to take care of cyber

attacks as quickly as possible, and increasing the likelihood of a payout[12]. Finally, modern warfare mainly takes place in cyberspace, with malignant forces aiming to take down industrial control systems (ICS) to create unrest amongst the civilian population and neutralize military response capabilities[11]. Due to the energy sector's importance, it is particularly targeted amongst all critical infrastructure sectors.

These risk factors continue to escalate in recent years. Since the advent of Bitcoin in 2012, ransomware use has been on an upward trend[6]. Moreover, the effects of the pandemic are compounding the growing threat; since many employees switched to a work from home model, companies reduced security measures to accommodate the change, leading to a rise in attacks[6]. Energy firms currently spend approximately 0.2% of their total revenue on cybersecurity[11], an alarmingly low figure considering the stakes. A study by the publication CSO found that 86% of companies have limited to no visibility into their ICS environments, 77% of companies have poor network segmentation, allowing easy movement from the IT network to the operational, or OT, network, and 44% of companies have shared user credentials between IT and OT networks, meaning anyone who obtains access to one network can use the same credentials to access the other network[12]. As digitalization of industry progresses, the surface area of attack rapidly expands, opening these essential providers to greater possibility of infiltration and disruption[11].

3. Research methods

The methods of research employed in this report began by studying the wide-reaching effects of the Colonial Pipeline ransomware attack in 2021. This pipeline supplies roughly half of all fuel to the East Coast, making it essential for mass transit and manufacturing in the region[13]. Since the effects of the halted pipeline were so tangible to everyday citizens, the attack was highly discussed in reputable news outlets for everyday civilians, such as the New York Times, and in specialized publications for topics in cyberspace. Many cybersecurity publications, including CyberCrime Magazine and US Cybersecurity Magazine, studied the failings of the Colonial Pipeline which allowed a ransomware group to easily manipulate an essential source of fuel.

The next source of research in this report comes from the government's response in the form of press releases, executive orders, and cybersecurity initiatives. The actions taken in the

public sector towards legislating cybersecurity directly influence change in the private sector, so federal solutions to this issue must be noted. The instructions from Biden's 2021 executive order and recommendations of the Solarium Commission, a conglomeration of both private and public experts in critical infrastructure, were collected. Finally, in order to review the efficacy of the public sector's actions, this report draws on the critiques and suggestions of academics in cybersecurity. The Journal of Cybersecurity and research collected by universities provide commentary on the steps that have been taken, and suggestions for improvement of cybersecurity in the energy sector moving forward.

4. Fortifying the energy sector against future cyber attacks

4.1 Colonial Pipeline Cybersecurity Failings

The ransomware attack mounted by the cybercrime group known as DarkSide against the Colonial Pipeline should not have caused a cease in operations. The company made a series of mistakes that allowed this to occur. To begin, Darkside was able to enter Colonial's IT network using stolen credentials, most likely acquired using phishing tactics. Darkside was then able to enter the network using an old VPN that was no longer in use, but was still connected to the network and unmonitored. Finally, Colonial did not employ Multi-Factor Authentication to prevent unauthorized access to their network[14].

Once inside the IT network, Darkside stole corporate data, then subsequently launched their "double extortion" ransomware attack, threatening to release the stolen data while also encrypting data still in the Colonial Pipeline systems[6]. The company then proceeded to shut down all operations, and though unknown at the time, the reason for this drastic response was the fear that DarkSide would, or had already infiltrated the pipeline's operational technology (OT) network[13]. The OT network controls the machinery that monitors and distributes fuel to customers, then sends that information to the IT network for billing[10]. Energy companies are expected to sequester their IT and OT networks to prevent malware spread[13], so the response in the Colonial Pipeline incident displayed serious deficits in the company's basic security measures and management.

4.2 Public Sector Cybersecurity Improvements

The responsibility for improvements largely belongs to private industry firms that control distribution, but it is the role of the government to regulate important aspects of our economy and set a precedent of security. Beyond internal reforms, the government must improve threat information sharing between private and public sectors. Communication flow must become faster and more widely used, in order to aid companies under attack and enable communication from experts[5]. The government has many agencies to address cyberthreats, such as CISA, DHS, and NIST, but should restructure this hierarchy, as the current "alphabet soup of agencies" overseeing cybersecurity creates confusion[6]. As cyberattacks become more commonplace, the government will need to maintain exemplary levels of security, particularly since they may need to more heavily regulate the private sector moving forward.

4.3 Private Sector Cybersecurity Improvements

Private sector energy providers have the most responsibility to reinforce their cybersecurity measures under the current level of oversight, which is quite minimal considering the importance of the product they provide. Energy industry operations frequently use a Supervisory Control and Data Acquisition system, or SCADA, to control and measure product distribution[15]. Since SCADA essentially controls flow of energy resources, measures to secure these systems including extensive mapping of systems, applying monitoring and detection of infiltration software in SCADA platforms, network segmentation, and frequent risk assessments, must be applied across all energy companies[15]. Under the umbrella of network segmentation, improvement of firewalls allows industry actors to separate malicious traffic from normal network traffic in ICS and SCADA systems[11]. Another aspect of network segmentation includes application whitelisting in SCADA servers, which allows entry only to explicitly approved applications, rather than attempting to identify and block entry of infinite possibilities of bad applications[11]. Finally, unidirectional gateways which allow flow of data between IT and OT networks, but prevent the transfer of information back to the source network, much like a database, should be implemented to fully secure segmentation[16].

5. Results

This report finds that the rate of improvement of industrial cybersecurity is lagging far behind the rate that threats in the cyberspace to ICS in the energy sector are expanding. In 2021 and in the wake of a series of attacks, the government made great strides towards raising standards of security, though the progress was long overdue. The public office must continue its work to insulate the nation's cyber connected industry systems. The private sector has a responsibility to review their cyber eco-systems from top to bottom, returning to basic principles of confidentiality, authentication, and segmentation. Considering the severe ramifications of attacks on critical energy infrastructure that have been experienced in the wake of the Colonial Pipeline attack and other recent, high-profile incidents, combined with rising global tensions, reinforcement of cybersecurity in these areas is of the utmost importance to national security. If these changes are not implemented expeditiously, the private sector will need to be more highly regulated by the federal government, to ensure that basic levels of cybersecurity are met.

6. Conclusion

As the pillars of modern society become ever more dependent on digitized power sources, the threat posed to citizens around the world increases proportionally, if not at a more rapid pace due to exponential technological advances. Private energy providers should study the failings of recent malware attacks on industrial systems, and ensure that they are not susceptible to repeating those same mistakes. Many of the recommended adjustments are basic measures that may be time-consuming to implement, but offer invaluable protection to the systems that power our economy and day to day life. Though the government has made progress towards a standardized level of cybersecurity in the US, individual companies must take action to fortify their cybersecurity and cyber resilience. Any chance for stable, civilized life in the constant inconsistency of the digital age relies on a dedication to increasing the nation's cybersecurity to protect the energy sector of our critical infrastructure.

References

1. Obama, B. (2013). Executive order 13636: Improving critical infrastructure cybersecurity. Federal Register, Vol. 78, Issue 33, 11739.
2. Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. Land Forces Academy Review, 26(1), 69-75.
3. Executive order on improving the nation's cybersecurity. (2021). Retrieved December 7, 2022, from https://www.cisa.gov/executive-order-improving-nations-cybersecurity
4. Statement from CISA acting director Wales on executive order to improve the nation's cybersecurity and protect Federal Networks. (2021). Retrieved December 7, 2022, from https://www.cisa.gov/news/2021/05/13/statement-cisa-acting-director-wales-executive-order-improve-nations-cybersecurity
5. Countering Cyber Threats to Critical Infrastructure: What's Next? (2021). In Carnegie Endowment Panel. Retrieved 2022, from https://www.youtube.com/watch?v=WFX3Vy08xLc
6. Dudley, R., & Golden, D. (2021). The Colonial Pipeline Ransomware Hackers had a Secret Weapon: Self-Promoting Cybersecurity Firms. ProPublica. Retrieved 2022, from https://www.propublica.org/article/the-colonial-pipeline-ransomware-hackers-had-a-secret-weapon-self-promoting-cybersecurity-firms
7. The White House. Executive Order on Improving the Nation's Cybersecurity. The United States Government, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.
8. CISA. Critical Infrastructure Sectors. Cybersecurity and Infrastructure Security Agency CISA, October 21, 2020. https://www.cisa.gov/critical-infrastructure-sectors.
9. Sanger, David E., and Nicole Perlroth. Pipeline Attack Yields Urgent Lessons about U.S. Cybersecurity. The New York Times. The New York Times, May 14, 2021. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.
10. Zetter, Kim. US Gov Issues Emergency Order While Colonial Pipeline Is Down. Zero Day, May 10, 2021. https://zetter.substack.com/p/biden-declares-state-of-emergency.

11. Aljohani, Tawfiq M. Cyberattacks on Energy Infrastructures: Modern War Weapons. arXiv.org. Cornell University, August 28, 2022. https://doi.org/10.48550/arXiv.2208.14225.
12. Mello, J. P., Jr. (2022, February 24). Ransomware is top attack vector on critical infrastructure. Retrieved December 7, 2022, from https://www.csoonline.com/article/3651370/ransomware-is-top-attack-vector-on-critical-infrastructure.html
13. Perlroth, N. (2021). Colonial pipeline paid 75 bitcoin, or roughly $5 million, to hackers. Retrieved December 7, 2022, from https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html
14. Hempel, G. (2022, April 25). Back to basics: The vulnerabilities you're overlooking. Retrieved December 7, 2022, from https://www.uscybersecurity.net/csmag/back-to-basics-the-vulnerabilities-youre-overlooking/
15. Cunningham, A. (2022, February 02). The machine industry and control systems: The National Security Risks with SCADA. Retrieved December 7, 2022, from https://www.uscybersecurity.net/csmag/the-machine-industry-and-control-systems-the-national-security-risks-with-scada/
16. CSRC Content. Unidirectional gateway - glossary: CSRC. Retrieved December 7, 2022, from https://csrc.nist.gov/glossary/term/unidirectional_gateway