American Energy Infrastructure

The United States is currently facing a national energy crisis that drastically affects the average American. Recent cyberattacks have demonstrated how vulnerable the United States energy infrastructure is. It is in the nation's best interest to address this issue because the effects could alter the American way of life.

The American power grid is based on desires from the late 1800s and its goal was to provide electricity to as many people as possible at the lowest cost. The main issue is the original power grid was designed to meet the demands of the early 1900s. The power grids have not been updated since the 1960s and consequently, the systems that run the power grids are outdated.

The International Society for Automation and Control Systems (ISA99) recorded 1300 incidents annually of power failure due to cyber attacks. The Aurora vulnerability was a well-documented vulnerability that demonstrated how outdated the generators are. In 2007, The Idaho National Laboratories conducted an experiment with a computer program to rapidly open and close the generator’s diesel circuit breakers. The breakers were out of phase and this event resulted in the generator exploding.

Americans on average consume about five to six times the amount of electricity as the average person. Today the United States power grid loses power three times more often than in the 1980s. The concept of predicting the rise in demand for power was not an idea that was thought at the time the grids were established. This negligence has ultimately led to the problem the United States is currently facing with its infrastructure.

Another way hackers can exploit America’s power grid is through backdoors configured in the hardware. There is a growing security concern from equipment purchased from foreign manufacturers. This equipment can often be found in the three main grids of the United States, the Eastern grid, the Western grid, and the Electric Reliability Council of Texas (ERCOT). In 2019, a Chinese-built transformer was seized from the Port of Houston by the Department of Energy and Homeland Security. For unspecified reasons, the transformer was taken to the Los Alamos Laboratories in New Mexico. It is suspected that there was a backdoor of electronics that could be used for malicious intent. Hackers could take control of the power grid operations or even dismantle the whole system. On May 1st 2020, President Trump signed an executive order that directed utilities to not purchase power equipment from adversaries to the United States.

There is a growing notion of securing the power grid in the United States. The integration of newer technology in the power systems raises a concern. When re-engineering a system there is a tradeoff in risk. The advantage of automating the power system, will improve performance and expand humanity's capabilities. However, many would argue the more automated the power system becomes, the more susceptible it can be to cyberattacks. Even though there is no clearly defined boundary, the engineers must take into consideration which components should be automated.

Another way to address the security concerns for the power systems is to create more accessible and reliable energy storage systems. Traditionally fossil fuel power plants are constructed far away from population centers, meaning the power needs to be transmitted long distances. This idea raises a reliability concern because there are now more variables to take into consideration to ensure the community receives power from a source. Ideally, if there were multiple power plants this could ensure continuous power in case one of the plants failed to deliver power. A smart grid could be implemented which would have the ability to send power from multiple sources. This could behave as a backup generator, and have an energy storage system in place to ensure the community receives power.

If the energy sources were diversified in a given area, this could also make it much more difficult for attackers to exploit the power grid. It would be much more different for an attacker to take down a coal power plant compared to a hydroelectric power dam. It would require more resources, time, and manpower to penetrate a power grid with varying sources. If the smart grid was configured to use these sources to act as an energy backup or storage, then it can give responders more time to address the attack without sacrificing essential power services.

On May 7th 2021, one of the largest pipelines experienced a cyberattack that shut down fuel delivery all over the southeast. The Colonial Pipeline spans about 5,500 miles and carries millions of gallons of fuel per day. The pipeline is essential to several industries on the eastern seaboard and is responsible for supplying fuel to airports along with military bases. This pipeline is vital for supplying oil, gas, jet fuel, and refined products throughout the east coast. Many Americans depend on the Colonial Pipeline to meet their daily fuel needs.

The Colonial Pipeline was shut down due to a cyberattack from a Russian hacker group known as DarkSide. The pipeline was a victim of a ransomware attack that took control of the pipeline's computer systems. The attack works with the ransomware encrypting a target's files with an encryption algorithm such as AES or RSA. The files become unreadable to the owner and typically the attackers hold the key to decrypt the files. Once the ransomware has encrypted everything, an extortion message is displayed, usually asking for payment in exchange for the key. The attackers would relinquish control of the systems if they were compensated 75 bitcoin, which is roughly five million dollars at the time.

According to Colonial, the company decided to shut down the pipeline to contain the threat. This resulted in one of the largest disruptions in American infrastructure by hackers in history. This in consequence raised fuel prices due to a lack of supply to meet a certain demand. This event triggered many Americans to panic buy, along with businesses shutting down.

The company didn't have many options to address the situation, especially since they had a limited amount of time before the consequences got dire. One option is to pay the hackers, but the company would not have any way of guaranteeing they will have control of their system after the transaction. This would also set a dangerous precedent for future ransomware attacks. Another option would be to address the attack, but this would be challenging since the company is under a time limit. This could have the potential to cause more damage if the business decided to take this approach since their services are essential to the public.

Colonial immediately notified government authorities including the FBI and the US Department of Energy. The company also cooperated with a third-party company known as FireEye, which specializes in preventing cyberattacks along with mitigating their effects. The systems that were affected by ransomware controlled the pipeline's operations along with both internal and external IT systems. It was also reported that the criminal group stole over 100 gigabytes of data from company servers. With government cooperation, there was a slow plan to resume the pipeline's operations, but it would take the time that many Americans could not afford. To make up for the fuel demand the government made temporary exceptions to waive rules on how long a truck driver could drive to deliver fuel.

When the FBI identified the hacker group known as DarkSide they concluded that the organization had no ties with the Russian government. It was believed that this group was apolitical, and the main motive was to make money. From their perspective, they believed that they are a gray hat hacking group which means they would cripple a target’s system for monetary gain, but expose vulnerabilities. It was believed the attackers were able to penetrate Colonial’s Information technology systems using employee profiles and passwords circulating on the dark web long before the attack was carried out. This is known because the group often shares how they would break into a system and how to prevent it. This as a result will expose a lot of their target's information to black hat hackers within the organization, who would use this opportunity to sell this kind of information to the highest bidders.

The group also has a reputation for honoring payments but has also leaked information online to discredit its victims. Colonial resolve this situation by paying the ransom to DarkSide which many experts believed set a dangerous precedent. Traditionally, these transactions are done with cryptocurrency since they are more likely to be untraceable, however the FBI was able to recover some of the funds. President Biden signed an executive order that would lay out stricter standards for any software sold to the United State government energy infrastructure along with an incident response team to review these major cyber attacks.

In February of 2022, the Russian Federation invaded Ukraine, which raised concerns about global security. The Russians decided to carry out cyberattacks against Ukrainian critical infrastructure before the invasion. The attacks consisted of attempts to spread malware throughout Ukraine’s critical infrastructure along with gathering important information. This issue made it much more difficult for the Ukrainians to defend against the invasion. Despite the world’s views about the ongoing conflict, Russian President Vladimir Putin announced that any nation that chooses to get

involved would have devastating consequences. Many nations decided to get involved in supporting the Ukrainians for political purposes including the United States.
The Department of Homeland Security issued a warning about the Russian government having the ability to carry out cyberattacks against critical infrastructure.

In March 2022, The Senate passed the strengthening American Cybersecurity act of 2022. This bill was introduced by Senator Rob Portman (R-OH) and Gary Peters (D-MI). President Joe Biden signed the bill into law with the intent to improve America's cyber security infrastructure response.

The law would mandate critical infrastructure operators to report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA). A cybersecurity incident must be reported within 72 hours of discovery. The act also requires ransomware payments to be reported within 24 hours of receiving a ransom payment demand. The report must cover a full description of the incident, a description of the vulnerability exploited, identifying all known parties along with their contact information, information that has been compromised, and providing notice. One of the problems with this law is it is not clear what business in critical infrastructure is considered to be covered entities, which raises an issue of what can be insured.

The law has also included some revisions that are intended to improve America's cyber security response. The law would improve cooperation with civilian federal government agencies. Agencies will be required to share certain information to improve the coordination of cyber security operations. Finally, the law would authorize the Federal Risk and Authorization Management Program to adopt cloud-based tech for five years to improve federal government operations. This legislation will help federal agencies to modernize and improve digital services for the American people.

In conclusion, the United States has historically brought the world some of the best innovations, however, has failed to keep them up to date. It is in an attacker's best interest to take down an essential service that their target relies on rather than attacking a victim specifically. In the modern world, many Americans depend on energy to carry out their everyday lives. It is imperative for this country to secure its energy infrastructure if it chooses to continue to be a world power.

References:

Cyber Attack Exposes Risk in America’s Energy Infrastructure: https://www.economist.com/united-states/2021/05/13/a-cyber-attack-exposes-risks-to-americas-energy-infrastructure

Colonial Pipeline: https://www.youtube.com/watch?v=qJM5zG9XhZ8

Attack Explained: https://www.youtube.com/watch?v=0g14ugtxniI

Securing America’s Energy Infrastructure: https://www.energy.gov/articles/securing-americas-energy-infrastructure-cyber-threats

Colonial Pipeline News: https://www.youtube.com/watch?v=kKsxnF20Zgs

President Biden warns Potential Cyber Threats on US infrastructure by Russian Forces: https://www.youtube.com/watch?v=KYf7BCUPDOI

Strengthening American Cybersecurity Act: https://www.dlapiper.com/en/us/insights/publications/2022/03/us-senate-unanimously-passes-the-strengthening-american-cybersecurity-act/

Strengthening American Cybersecurity Act: https://www.onetrust.com/blog/strengthening-american-cybersecurity-act/

Ransomware: https://www.youtube.com/watch?v=YRwEjeFv99k

Russia State Sponsored Cyber Criminals: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

America’s Energy Dependencies: https://www.eia.gov/energyexplained/us-energy-facts/imports-and-exports.php

Securing America's Energy Infrastructure: https://www.energy.gov/articles/securing-americas-energy-infrastructure-cyber-threats

Cyber Attacks Against Energy Infrastructure: https://news.climate.columbia.edu/2022/04/01/the-risk-of-russian-cyberattacks-on-us-energy-infrastructure/