CYBER SECURITY & INFO TECHNOLOGIES

Rethinking Cybersecurity after Colonial Pipeline Hack

JULY 23, 2021

Download PDF

The debate over the nation's preparedness for cyberattacks is still raging two months after the Colonial Pipeline hack which gave a heads-up about the vulnerabilities of the critical infrastructure to malicious cyber actors. The incident sparked growing concerns across the country about cyber threats to national security and our society.

The ransomware used in the attack, FBI says, is developed by an allegedly Russia-linked hacker group called Darkside. Ransomware is a form of malware designed to encrypt files on a computer, rendering those files unusable. Cybercriminals then demand ransom to be paid in cryptocurrency in exchange for the decryption key. Ransomware is the fastest-growing cyber-crime threat in recent years. Although not a new phenomenon, it is becoming one of the most popular and profitable types of cyberattacks. This last attack is considered to be the largest ransomware attack targeting critical infrastructure.

High-profile targeted cyberattacks are generally carried out by sophisticated hacker groups, some of which are allegedly sponsored by foreign governments. Hackers behind the devastating SolarWinds data breach, which was revealed in December 2020, were reported to have links with Russia. The hacker group that developed the ransomware used in the Colonial Pipeline attack also has roots in Russia. Although there is no evidence suggesting that the Russian government was behind the pipeline attack, as President Biden said in a press briefing, experts pointed out that Russia provides a safe haven for cybercriminals and turns a blind eye to the activities of malicious hacker groups.

It is not only Russian hackers who receive media attention; Chinese hacker groups also perpetrated many cyberattacks aiming at U.S. targets. Recently, a cybersecurity firm, FireEye, discovered that allegedly state-backed Chinese hackers exploited vulnerabilities in remote access software used by government agencies, critical infrastructure, and the private sector in the US and Europe, suggesting a cyber espionage operation.

These attacks may or may not be sponsored by foreign governments. What matters most is that there is a trend in which cyberattacks are becoming more destructive and impacting the daily lives of citizens. Such attacks not only affect the economy, but they had serious political and social consequences for American society. For instance, the continuity and the volume of the damage caused by these attacks could lead to a decline in public trust in government. Russian interference in the national elections and subsequent social media disinformation campaigns have already damaged part of the public's faith in the democratic process. America's increasing vulnerabilities to foreign interferences, particularly in the cybersphere, could further entrench political divisiveness.

The SolarWinds hack was expected to serve as a catalyst to rethink the nation's cybersecurity at the federal level. Experts argue that the current system is broken and there is a need for organizational reform. After the SolarWinds hack, the Biden administration has vowed to make cybersecurity a top priority. The last Colonial Pipeline hack clearly demonstrated the urgency to act to modernize the nation's cybersecurity in order to respond to highly sophisticated attacks against critical infrastructure.

President Joe Biden signed an executive order addressing the security of the federal computer networks after the ransomware attack targeted the Colonial Pipeline. The order introduced some measures to modernize the country's cybersecurity. The order acknowledges the growing threat of malicious cyber campaigns and emphasizes the necessity of a partnership with the private sector to improve the cybersecurity infrastructure. It also brings some extra measures to be taken by federal institutions in order to prevent and mitigate cyberattacks. This step is an indication that the administration takes cybersecurity very seriously.

The private sector operates most of the nation's critical infrastructure. Cybersecurity vulnerabilities that could exist in these systems are clearly matters of national security. A Bloomberg report reveals that the U.S. Transportation Security Administration's Pipeline Security Branch which is responsible for protecting the nation's pipelines does not enforce mandatory requirements for cybersecurity, instead relies on discretionary protection. When there are no enforced mandates, companies could be reluctant to spend money on improving their cybersecurity infrastructure or allocate more resources.

There is no simple solution or quick fix in this area. The public-private partnership has always been the motto for any discussion to address the challenges. However, given the sophistication and expansive impact of the recent attacks and clear indications about the desires of the malicious actors to engage in similar attacks, there is a need to redefine the public and private partnership to improve cybersecurity and critical infrastructure.

Starting with how we define the risks and vulnerabilities and taking further steps toward a more proactive cybersecurity approach, we can enhance the national cybersecurity posture. By being more open to cooperation and collaboration, public and private sectors can complement and support each other's efforts in dealing with cyber threats.

Political leaders are expected to work together to stand against cyberattacks. The Colonial Pipeline hack can be taken as an opportunity to ask ourselves the "what went wrong?" question and use the answers to come up with more effective security measures and mechanisms.
