An Analysis of Critical Infrastructure: Government Facilities

Written By: Altamash Ali

Publication Date: April 23, 2021

In recent years, the US has suffered from a dramatic increase in cyber-attacks originating from outside the US. Attackers often range from nation-states to criminal organizations, each with different goals in mind. The most dangerous attacks, however, have come from nation-states which possess the resources to carry out large-scale attacks on critical infrastructure. The Patriot Act defines critical infrastructure as systems and assets vital to the United States such that the destruction of such systems and assets would have a debilitating impact on security and national public safety [1]. Recent attacks on critical infrastructure, which have disproportionately affected government facilities and agencies, have exposed fundamental vulnerabilities in our current system of governance and have pressured authorities to reassess their defense mechanisms and plans for incident response.

On December 13, 2020, it was disclosed that several government facilities were the victims of an ongoing data breach which had began as early as March 2020. It is believed that a group associated with Russian intelligence had planted malware in a routine software upgrade from SolarWinds, a network-management company which provides services to government entities such as The Treasury Department, The Justice Department, and even nuclear facilities [2]. This resulted in the hackers being able to gain unauthorized access into government networks and snoop around for months on end while remaining undetected, something which was completely uncalled for. The sheer complexity and sophistication of such an operation has served as a wake-up for many experts and forced them to reevaluate the scope of the dangers we may face. What the current administration is more concerned about is why both the intelligence community and federal agencies, such as CISA, had failed to identify the attack [3]. This prompted a legal discourse on two fronts: how did our defense mechanisms fail and how should we respond?

Issues related to critical infrastructure are difficult to address in the US where much of it is privately owned. In addition, the growth of the Internet of Things has also made addressing these issues increasingly complex. Given that it isn’t very efficient for the government to develop hardware and software solutions in-house, they end up outsourcing services and buying products from trusted third-party vendors. When you come to realize that every router, every software program, and every industrial controller, sold by each of their numerous vendors, may each come with their own inadvertent backdoor or vulnerability, it is not hard to see the depths to which the government may have to go to administer compliance checks over their critical

infrastructure. Given that the vendors which the government purchases from are largely privately-owned, it is much more difficult to administer quality assurance reviews which are up to par with what should be required for national security. It also seems that despite the existence of government frameworks and regulations such as NIST controls, FIPS 140, and SOX compliance, outside attacks ensue. The attack on SolarWinds only serves to further delegitimize the effect these standards are having. According to Tom Bossert, former Director of Homeland Security, "A 'do over' is mandatory and entire new networks need to be built – and isolated from compromised networks" [2]. Joe Biden has proposed that $10 billion in the $1.9 trillion stimulus package be allocated for cybersecurity. In addition, Congress is looking to include $1 billion for the Technology Modernization Fund in the relief bill [3]. Now while this is a great investment for our future, we still need to address the ever-looming threat realized by the SolarWinds attack.

Attacks in the digital realm are much harder to define and label compared to attacks in the physical world. CISA is working to evaluate underlying frameworks to identify the scope of this breach and determine what type of response it should constitute. Since such frameworks are merely just frameworks and cannot quantify ever possible scenario, determining the legality of the matter usually depends on the terminology and principles outlined in years prior. The issue with this is that since technology is an ever-evolving landscape, what may constitute an attack one year may just be brushed off as espionage another year. It seems that lagging congressional legislature and a lack of importance placed on cybersecurity issues has been, in part, responsible for the failure to properly address such attacks on critical infrastructure. Once again, the destruction or derailment of such critical structure can have a debilitating impact on security, national economic security, as well as national public health or safety [1]. This is why, in the face of ongoing attacks from nation-states on government facilities, stricter and more definitive legal guidance is necessary in ensuring our nation's security.

Upon analysis of recent attacks, it seems that infirm hardware and software governance combined with the explosive growth of the Internet landscape have been the primary point of failure for government facilities. Had there been stricter legal precedence and prioritization of cybersecurity issues in the years prior, such a damaging outcome could have been avoided. In the words of President Biden, "we have to be able to innovate, to reimagine our defenses against growing threats in new realms like cyberspace."

Sources

[1] http://www.law.cornell.edu/uscode/text/42/5195c

[2] https://www.newyorker.com/news/daily-comment/after-the-solarwinds-hack-we-have-no-idea-what-cyber-dangers-we-face

[3] https://www.cfr.org/article/why-solarwinds-hack-wake-call