Memorandum for Rep. Canduit

Nicholas Robertson

CYSE 406

November 29, 2023

Noteworthy Cybersecurity bills/laws

In my research I have found that there have been a lot of noteworthy bills and laws that have both passed and have failed regarding cybersecurity practices and standards. A few highlights in my investigation would be the Intergovernmental Cybersecurity Information Sharing Act which according to GovInfo.gov, was created on Monday, December 5, 2022. The Act has not been approved by the federal government, but it has been proposed to the house and it is designed to tackle the issue of communication between branches of the government and how information about cyber attacks are shared in order to make it easier for cybersecurity departments within these different branches to work together more seamlessly, so that federal systems and networks are better protected. So, if an attack was launched against a branch of government, it will connect the federal governments cyber division with other private divisions that work under the government, so that information can pass through the supply chain much faster. Another one is the Better Cybercrimes Metric Act, which was sent to the house on March 28th, 2022, and passed by President Joe Biden on May 5th, 2022. It is designed to "require the FIB to integrate cybercrime incidents not its current reporting streams to better understand all the types of crime that Americans face" (Brian Schatz, 2022). This will help the government in the future in giving them some sort of normality, in how to respond and prevent cyberattacks. However, asides from those two examples, there is one Legislation that stands out, due to its in-depth focus on cybersecurity, which is the Cyber Incident reporting for Critical Infrastructure Act of 2022.

The Cyber Incident Reporting for Critical Infrastructure Act

This Act has been signed into law by President Joe Biden since March of 2022. The purpose of this law is to make sure that when a cyber-attack (most notably, ransomware attack) is launched on one of our countries critical infrastructures (i.e., gas pipeline, electrical grid, etc.), then "the law requires critical infrastructure entities and federal agencies to report significant cyber incidents and ransomware payments to the DHS's Cybersecurity and Infrastructure Security Agency (CISA) no later than 72 hours after the cover entities reasonably believes that the covered cyber incident has occurred." (CSO, 2022). It also specifies that if a payment was made in an attempt to get rid of the ransomware attack, then the organization that paid the

ransom, must report it to law enforcement within a 24-hour time frame as well. As stated in the on page 156 of the Federal Register/ Vol. 87, No. 175 on Monday, September 12, 2022, “Timely reporting of incidents also allows CISA to share information about indicators of compromise, tactics, techniques, procedures, and best practices to reduce the risk of a cyber incident propagating within and across sectors.” (Office of the Federal Register, 2022). This statement is basically saying that, with the proper information on cybercrimes and attacks on critical infrastructure, the better the chances of them relaying that information across to different agencies and cybersecurity branches.

History of this law

This law was made as response to the rapid cyberattacks that were taking place within critical infrastructure around that time. While cyberattacks happen on a daily basis, this law came into development off the heels of two back-to-back cyberattacks that took place on America’s critical infrastructure. These attacks being the Solar winds attack, which was a supply chain attack on government organizations that was using the infrastructure monitoring and management software, Orion, in order to make a undetected backdoor (a undetected access point on someone’s computer/network) into their networks, to steal valuable information from the government. The other attack was the colonial pipeline attack that took place from May 6, 2021 – May 12, 2021. This was a ransomware attack that effect tens of millions of people from Texas, the gulf and up the east coast.

What this law hopes to fix

While these two incidents might be the main driving point behind this law being passed, they are not the only reason for why it was passed. If you notice, this law puts heavy enfaces on the concept of reporting an attack that has taken place. This is because, a lot of attacks that are conducted on these organizations are never reported to the FBI, or any other government agency. The reason for this is due to how difficult it is to catch these criminals, even for the government. This makes it to where the companies believe that it’s a waste of time for them to report the attack, and they believe that it would be easier to just pay the ransom and move on. The biggest

inconvenience that an attack can have on any company, is wasting their time, because production is at a standstill. The more time that is wasted, the more money they loss in the process and for the majority of these companies, they will typically pay the ransom, in the hopes of getting back in operations as soon as possible. While this is an understandable viewpoint on the side of the corporations, there are consequences for a decision like this. This being that the FBI has no records of an attack on a critical infrastructure even happening. This makes it hard, if not impossible to prepare, warn other companies from similar attacks in time or even know how handle attacks like these in the future, due to the lack of records of these attacks happen. This law was made to fix the issue of lack of data on how frequent these attacks tend to happen. In other words, this law will help give the government a more consistent pattern on the types of attacks that happens along with how frequently these attacks tend to happen on these critical infrastructures.

Suggested Improvements

Overall, this law covers all of its bases, and there are not a lot of improvements that you can make to this law, that hasn't already been outlined in the law itself. But if I had to nitpick, I would suggest harsher penalties/punishment for the companies that doesn't report attacks on their companies, to bypass government intervention. I believe that even if this is an all-around reasonable law to follow, there are stilling going to be companies out there that will refuse to cooperate with the government, under fear that the government might find that there may be some shady business taking place behind the scenes of their own business. In order to prevent this, there should be an outline, stating the punishments that they would be faced with, if they don't comply. They could outline that, not complying with this law, could result in millions of dollars' worth of fines and up to jail time for the higher ups in these companies' CEO's and executives. This would seem reasonable, as these attacks on critical infrastructure, can seriously put individuals lives in danger, if its not reported in.

Final Thoughts

Rep. Canduit I believe that this is a great law that may give voters insight to how the process of cybersecurity attacks works, as well as giving them insight in how the government handles attacks like this. This can also give the people more confidence in the government, with regard to how they handle attacks on infrastructure that we use to help live. It is important to inform the pubic about these cyberattacks on their critical infrastructure in an informed and subtle way without causing and panic. It is also important that this law is passed so that the government is more informed about the attacks that are happing on these infrastructures every day. With the combined knowledge and information, we have about these attacks the government will be able to warn other critical infrastructure companies before they are attack, which will reduce the likely hood of them being a victim of the similar if not the same type of attack. This is not only a big step in the right direction for the government, but this is also a big step for cybersecurity, as the issue of cyberattacks will be taken much more seriously in the future.

Quotes

Cynthia Brumfield (June 07, 2022). "*U.S. cybersecurity congressional outlook for the rest of 2022"*

https://www.csoonline.com/article/572889/u-s-cybersecurity-congressional-outlook-for-the-rest-of-2022.html

Office of The Federal Register (September 12, 2022). "*Federal Register / Vol. 87, No. 175*

https://www.govinfo.gov/content/pkg/FR-2022-09-12/pdf/FR-2022-09-12.pdf

"Schatz Legislation to help fight cybercrime signed into Law" (March 05, 2022) Brian Schatz

https://www.schatz.senate.gov/news/press-releases/schatz-legislation-to-help-fight-cybercrime-signed-into-law