Austin Cupp Research Memo 6/11/2022

Purpose:

Hello Mr. Canduit, the purpose of this memo is to highlight a proposed legislation that has been passed by the United States Senate, and is now at your United States House of Representatives that involves companies and organizations under the critical infrastructure sectors such as tunnels, railways, bridges, healthcare, agriculture, nuclear reactors, and transportation that experience a significant cybersecurity incident to report it to the proper agency within a 72-hour time frame or those that experience a ransomware attack are to report it to the proper agency within a 24-hour timeframe.

Background about legislation:

Mr. Canduit, recently the United States Senate unanimously passed a new bill that is called SACA, which is the Strengthening American Cybersecurity Act of 2022. As it awaits its fate at the United States House of Representatives, I figured it would be important to discuss key points of the legislation. The main purpose of this bill is to, as mentioned, require companies and organizations that fall under critical infrastructure to report a major cybersecurity event, such as a security breach, or an attack for example, to the CISA (Cybersecurity and Infrastructure Security Agency) within a 72-hour timeframe and also to report any ransom payment demand within a 24-hour timeframe. This means that they, through FedRAMP, are to assess whether or not the risk is severe enough to notify whoever is affected by the event, and if it is deemed severe enough, provide those affected with a written notice. Also, a description of the cyber incident or ransomware attack is expected, which would include identifying the affected networks, devices, and systems, what specific unauthorized access occurred, and the time range the incident occurred as well as the overall effect the incident had on operations. The legislation also includes other reforms that are intended to help strengthen cybersecurity internally within the federal government. Some of those reforms include civilian agencies must also report any large-scale cyber event to the CISA in the 72-hour time frame as well, federal agencies are required to share information amongst one another to help improve coordination between them, and authorizing for 5 years, FedRAMP, which is the Federal Risk and Authorization Management Program that is also within the General Services Administration (GSA). Ransomware attacks can be very damaging, so a task force was created against these attacks. Also, a startup program was enacted to help determine what specific identity information systems could be vulnerable to cyber security events.

Final observations:

Overall Mr. Canduit, the legislations' main goal is to strengthen cybersecurity within the federal government and critical infrastructure as well as report incidents that could be harmful to the government and the public. Voters want laws that will give them a peace of mind that their information is protected, but let's say if a cybersecurity incident were to occur, they would know that one did indeed occur, and they would know that the entity that caused the incident would face proper consequences. As of right now, there is no legislation that would require those affected by a cyber incident to notify the CISA about what happened, what information was compromised, and who all was affected by the incident. If the discussed legislation were to be passed, it would, as mentioned, give the voters and those within the industry a piece of mind about the overall current state of cybersecurity and their information. However, one improvement that could be made to the aforementioned legislation is enacting consequences to those who do not properly disclose that they experienced a cybersecurity

incident, as well as reducing the timeframe for reporting the incident from 72 hours to 48 hours. Otherwise, I think the legislation is ready to be passed, and would be gladly welcomed by the public and government agencies.

Sources

"U.S. Senate Unanimously Passes Cybersecurity Legislation Requiring 72 Hour Cyber Incident Notification." (2022, March 17). *Natlawreview*. Hunton Andrews Kurth LLP, 2022. https://www.natlawreview.com/article/us-senate-unanimously-passes-cybersecurity-legislation-requiring-72-hour-cyber#:~:text=U.S.%20Senate%20Unanimously%20Passes%20Cybersecurity%20Legislation%20Requiring%2072%20Hour%20Cyber%20Incident%20Notification&text=On%20March%202%2C%202022%2C%20the,or%20the%20%E2%80%9CBill%E2%80%9D).

Franklin, Z., & Ganow, S. "Strengthening American Cybersecurity Act of 2022." (2022, April 8). *Lexology.* Taft Stettinius & Hollister LLP, 2022. https://www.lexology.com/library/detail.aspx?g=cdc5fdd0-6968-4d70-b0b7-d96278c4cbe0#:~:text=One%20broad%20interpretation%20of%20the,healthcare%20and%20public%20health%20sector.

Serwin, A., Meshulam, D., McAndrew, E., & Javanshir L. (14, March 2022). "US Senate Unanimously passes the Strengthening American Cybersecurity Act." *DLApiper*. DLA Piper LLP, 2022. https://www.dlapiper.com/en/us/insights/publications/2022/03/us-senate-unanimously-passes-the-strengthening-american-cybersecurity-act/

"All Information (Except Text) for S.3600 – Strengthening American Cybersecurity Act of 2022." (2022). *Congress.gov*. https://www.congress.gov/bill/117th-congress/senate-bill/3600/all-info