Political Implications of Cybersecurity Policy

Adam Johnson

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Professor: Bora Aslan

October 2, 2022

When it comes to creating and enforcing Cybersecurity Policy, there is a big difference in the private and public sector. The federal government doesn't pay as well as the private sector and has a hard time maintaining the appropriate talent required to advance policies and stay ahead of attackers. Politicians tend to link cybersecurity policy to events and propose legislation based on discovery of information or regulation instead of as a preventative measure. In the past year many of the legislative proposals have to do with regulating cryptocurrency and incident reporting. The Congress and Senate have been able to allocate and pass cybersecurity funding bills but have a hard time passing anything concrete in cybersecurity policy. Tom Leithauser quotes in his policy report that "A large cyber budget does not necessarily translate to better cybersecurity, nor is it an effective risk metric, as it is difficult to distinguish if budgets are appropriately funded. Substantial budgets can be indicative of a larger attack surface, an inefficient use of resources or higher reliance on legacy technology"(Fitch 2022). The government seems to have been taking a slow approach to addressing these problems since they are trying to deal with putting federal guidelines on the private sector. Sen. Ron Johnson (R-Wis.), who was the chairman of the Homeland Security committee in 2020 said "we have to look to the private sector because the private sector is always going to outperform the government"(Lee, 2020). Sen Johnson is also quoted as saying "The federal government has a really difficult time attracting, hiring and retaining the best talent, they just can't pay for it"(Lee, 2020). The federal government does not pay as much as the private sector does for cybersecurity specialists and this puts most of the talent and resources being used to protect private corporations.

Some recent cybersecurity policy advancements have come from presidential executive orders or national security memorandums. The most recent advancement in cybersecurity policies for policymakers was the “Cyber Incident Reporting for Critical Infrastructure Act”(CIRCIA), which was signed into law in March of this year. CIRCIA was introduced by Sen. Gary Peters (D-MI) and Sen. Rob Portman (R-OH) in september of 2021. When commenting on the bill Sen. Peters stated “When entities, such as critical infrastructure owners and operators, fall victim to network breaches or pay hackers to unlock their systems, they must notify the federal government so we can warn others, prepare for the potential impacts, and help prevent other widespread attacks"(U.S Senate 2021). The private sector controls the majority of infrastructure and cybersecurity related operations in the United States, so cooperation between the federal government and private sector are essential to make progress in national security and advancements of cybersecurity policy. When attackers target a privately owned business, or even infrastructure it may or may not be reported or reach the level of policymakers. The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) adds a requirement for private companies to report attacks which also includes ransomware. In the past a company who is the target of a major cyber attack or ransomware may not report the incident to law enforcement unless the information being compromised concerns national security or affects privacy acts such as HIPAA. If the attacks are reported the companies could lose investors or customers, so they may choose to avoid media coverage and not report the attacks. This could even mean paying out to ransomware attacks to avoid losses to business and minimize losses. But, now the private companies will be required to report certain incidents, even payouts of ransomware to the federal government within certain time frames. This allows the government to stay on top of the types

of attacks that are happening and help the federal government and other systems throughout the USA be aware and prepare for attacks following the same approaches. Some may question this level of political involvement in private business but the Fitch report states "Regulation is viewed as supportive of ratings, as it increases oversight and establishes a minimum budget for compliance and a floor for cyber hygiene" (Fitch 2020).

Since policy makers have had a hard time passing cybersecurity policies and acknowledging the big divide in private and public cyber operations, Senator Mark Warner from VA started the "cyber caucus". The caucus is focused on educating policymakers and the public about cybersecurity. Warner also authored the "Strengthening American Cybersecurity Act of 2022" which is another step in requiring companies that are responsible for critical infrastructure to report cybersecurity incidents to the federal government agencies such as CISA. In Tom's policy report journal, he notes that Fitch comments on these new government actions stating, "Cyber incident reporting rules and other cybersecurity regulation will boost the creditworthiness of private-sector entities, particularly critical infrastructure operators, by improving the cyber defenses of those entities" (Fitch 2022).

References

Leithauser, T. (2022). Fitch: Cyber Regulation Will Boost Business's Creditworthiness. Cybersecurity Policy Report , 1.

Congressional Research Service Releases Cybersecurity Assessment. (2021). Journal of Internet Law, 25(2), 3–16.

Lohrmann, D. (2022). Finding Common Ground: Election security has become a contentious issue, but there are a few matters both sides of the aisle can agree on. Government Technology, 35(5), 66.

Lee. H, (2020) Sen. Ron Johnson: Federal Government Needs to Partner with Private Sector for Cybersecurity https://www.theepochtimes.com/sen-ron-johnson-federal-government-needs-to-partner-with-private-sector-for-cybersecurity_3631001.html

U.S. Senate Committee on Homeland Security and Governmental Affairs, 2021. Peters and Portman Introduce Bipartisan Legislation Requiring Critical Infrastructure Entities to Report Cyber-Attacks. https://www.hsgac.senate.gov/media/majority-media/peters-and-portman-introduce-bipartisan-legislation-requiring-critical-infrastructure-entities-to-report-cyber-attacks

Warner M. (2022). Warner Applauds Senate passage of bipartisan cyber incident reporting legislation https://www.warner.senate.gov/public/index.cfm/2022/3/warner-applauds-senate-passage-of-bipartisan-cyber-incident-reporting-legislation