Garrett Moison
CYSE 425W – Policy Analysis 1
October 21, 2021

The U.S. Government's Strategy for Information Sharing to Improve Cybersecurity

Introduction

Security breaches cause immense financial and operational damage to organizations, decreasing their market value and reputation. As a result, organizations are compelled to invest in cybersecurity to prevent their physical and digital assets from being stolen or destroyed. Moreover, the volume and complexity of cybersecurity incidents have increased significantly in the last few years, forcing the need for new developments in security (Fuentes et al., 2016). While cybersecurity is still an ever-growing field, this paper will analyze the U.S. government's strategy to use information sharing to improve cybersecurity.

Overview

The U.S. Government's primary information-sharing strategy, the Cybersecurity Information Sharing Act (CISA) of 2015, was passed by the U.S. Senate. This act introduced the sharing of classified cyber threat indicators (CTIs) and defensive measures with private entities, federal agencies like the Federal Bureau of Investigations (FBI) and the Department of Homeland Security (DHS), and the Information Sharing and Analysis Center (ISAC) (Yang et al., 2020). Restricting access to specific, high-ranking government agencies lessens the chance of shared public and private data landing in the wrong hands. Furthermore, those departments and agencies are required to develop and publicize procedures to promote the sharing of (Yang et al., 2020):

1) "Classified and declassified cyber threat indicators in possession of the federal government with private entities, nonfederal government agencies, or state, tribal, or local government.

2) Unclassified indicators with the public.
3) Information with entities under cybersecurity threats to prevent or mitigate adverse effects.
4) Cybersecurity best practices with attention to the challenges faced by small businesses."

One of the most significant issues with the current legislation is its implementation. Even with the U.S. Government's support by sharing cybersecurity information, U.S. firms are not obligated to share theirs. Surveys done by cybersecurity officers reveal that while larger firms are more engaged with information sharing, smaller firms tend to keep theirs private (Yang et al., 2020). Likewise, organizations are not required to implement cybersecurity in their workplace, heightening the chance for cyberattacks.

Reason for Development

Following the rise in the number and complexity of cybersecurity incidents, Intrusion Detection Systems (IDSs) have gotten extensive research attention. However, isolated IDSs can be ineffective against coordinated attacks since their traces are spread across different domains (Fuentes et al., 2016). According to Fuentes et al., a solution to this problem is the collaboration between entities to help detect those attacks. Moreover, mechanisms for timely sharing actionable cybersecurity information such as vulnerabilities, detection signatures, or indicators of compromise are vital assets to share with others to avoid similar attacks. Newly developed approaches aim to facilitate automatic sharing through protocols (Fuentes et al., 2016). Although organizations have seen clear financial benefits and better security from information sharing, they refuse to share theirs out of a lack of trust. Nonetheless, with no strict requirement for implementing cybersecurity or sharing cybersecurity information, data on many attacks will not be shared with others, allowing them to strike again.

How this Strategy Fits Within a National Cybersecurity Policy

In an effort to combat the growing threat of cyberattacks, former President Obama issued an executive order in February of 2013 to strengthen the cybersecurity of critical infrastructure by increasing information sharing between private companies and the federal government regarding cyberthreats and breaches (Rodin, 2015). Furthermore, the National Institute of Standards and Technology (NIST) was directed to create a cybersecurity framework intended to "establish risk-based security standards for all companies that own or operate critical infrastructure" (Rodin, 2015). However, compliance with the order leads to the likelihood of more regulations in the future, becoming an issue for companies contracting with the government. For instance, the government could penalize contractors that disclose negative past performance regarding cyber-intrusions, decreasing their chances of obtaining future contracts (Rodin, 2015). Under certain circumstances, this is unfair, as many attacks can be out of a cybersecurity specialist's control. Currently, no effective national cybersecurity policy focusing on information sharing has been proposed.

Works Cited

De Fuentes, J. M., González-Manzano, L., Tapiador, J., & Peris-Lopez, P. (2016, December 27). PRACIS: Privacy-Preserving And Aggregatable Cybersecurity Information Sharing. *Computers & Security*. https://www.sciencedirect.com/science/article/pii/S0167404816301821.

Rodin, D. N. (2015). The Cybersecurity Partnership: A Proposal For Cyberthreat Information Sharing Between Contractors And The Federal Government. *Public Contract Law Journal*. https://www.jstor.org/stable/26419479.

Yang, A., Kwon, Y. J., & Lee, S.-Y. T. (2020, August 13). The Impact of Information Sharing Legislation on Cybersecurity Industry. *Industrial Management & Data Systems*. https://www-emerald-com.proxy.lib.odu.edu/insight/content/doi/10.1108/IMDS-10-2019-0536/full/html.