Information Sharing in Cybersecurity: Should Organizations Be Forced To Share Attacks?

Michael A Gurule

Old Dominion University

CYSE425W: Cyber Strategy and Policy

Bora Aslan

11FEB2024

Information Sharing in Cybersecurity: Should Organizations Be Forced To Share Attacks?

Cybersecurity has emerged as one of the most discussed topics as threats continue to rise. One conversation among those is the exchange of information, specifically threat related, among entities, both private and public. Many organizations, including the MITRE Corporation and ENISA (European Network and Information Security Agency), have already begun to facilitate information exchange through standards and initiatives. (Dandurand & Serrano, 2013) Others, such as NIST (National Institute of Standards and Technology) and ITU-T (International Telecommunication Union's Telecommunication Standardization Sector), have called for a central coordinated information exchange center. (Skopik, Settanni, & Fiedler, 2016) The U.S. Securities and Exchange Commission (SEC) has made a step forward with the addition of new rules governing reporting of incidents by all public companies in its domain. This paper will focus on the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure implemented by the SEC in the Securities Exchange Act of 1934 (the "Exchange Act").

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

The SEC implemented new regulations on July 26, 2023, aiming to improve disclosures regarding cybersecurity risk management, strategy, governance, and cyber incidents among public companies governed by the Exchange Act. In essence, this aims to enhance cybersecurity reporting across all public companies. The main component that comes with the new rules is the requirement to disclose all "material" cybersecurity incidents. (U.S. Securities and Exchange Commission, 2023) Brown et al. (2023) aid in the understanding of the word material in this context. There is no quantitative threshold for a cyber incident to be considered material. There are only examples given by the SEC that range widely from "a substantial likelihood that a reasonable shareholder would consider it important," to more abstract ideas like if the incident is

currently, or will harm the company's reputation, customer or vendor relations, or competitiveness (Brown et al., 2023).

Following the new rules, the addition of Item 1.05 on form 8-K (a report to the SEC) was implemented. Now this reporting form has in it the requirements for reporting. Some key information from this form is that the cybersecurity incident must be "determined by the registrant to be material" (Securities and Exchange Commission, 2023). This would mean that it is up to the company to determine whether the incident was material or not. Another very important aspect of the form to encourage disclosure of incidents is Item 1.05, Instructions to Item 1.05 (4), which states:

> A registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident. (Securities and Exchange Commission, 2023)

This very important sentence gives companies some leeway to control the amount of information disseminated about ongoing response. This also allows companies to give a detailed report of the incident without having to disclose important or proprietary information about systems and capabilities they control.

Conclusion

The Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure is a much-needed set of rules to bring about a better future for all those that traverse the cyber world. Trautman & Newman (2022) commend the SEC for moving in the right direction with these additional rules. Incident information sharing is of vital importance and can reduce the risk of

cyber-attacks to those participating by 50% (Safitra & Fakhrurroja, 2023). This addition of rules and requirements is recent and, hopefully, is the steppingstone to increasing cyber incident collaboration among all public and private organizations.

References

Brown, M. L., Muhlendorf, K. B., Scott, K. E., Brown, J. F., Garriott, B., & Quigley, J. M. (2023, August 1). *SEC adopts controversial New Cybersecurity Disclosure Rules for Public Companies*. Wiley Law. https://www.wiley.law/alert-SEC-Adopts-Controversial-New-Cybersecurity-Disclosure-Rules-for-Public-Companies

Bueno, F., Kanyeka, N., Kennis, G., Kolbe, P., Sady-Kennedy, A., & Zabierek, L. (2021). Toward a collaborative cyber defense and enhanced threat intelligence structure. *The Cyber Project*.

Chen, J., Henry, E., & Jiang, X. (2023). Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach. *Journal of Business Ethics*, *187*(1), 199-224. https://doi.org/10.1007/s10551-022-05107-z

Dandurand, L., & Serrano, O. S. (2013, 4-7 June 2013). Towards improved cyber security information sharing. 2013 5th International Conference on Cyber Conflict (CYCON 2013),

The Federal Register. 17 CFR 229.106. (2023, August 4). https://www.ecfr.gov/current/title-17/section-229.106

Trautman, Lawrence J. and Newman, Neal F., A Proposed SEC Cyber Data Disclosure Advisory Commission (April 29, 2022). Securities Regulation Law Journal, Fall 2022, pp. 199-234, Texas A&M University School of Law Legal Studies Research Paper No. 22-22, Available at SSRN: https://ssrn.com/abstract=4097138 or http://dx.doi.org/10.2139/ssrn.4097138

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, *15*(18).

Securities and Exchange Commission, Form 8-K: Current report purusant SIC to Section 13 or 15 (d) of the Securities Exchange Act of 1934, May 19, 1983 (2023). Washington, D.C.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154-176. https://doi.org/https://doi.org/10.1016/j.cose.2016.04.003

U.S. Securities and Exchange Commission. (2023, November 14). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. https://www.sec.gov/corpfin/secg-cybersecurity#_ftn2