How effective is the NIST Cybersecurity Framework 2.0

CYSE 425W

Danny Choi

August 04, 2025

Introduction

Cyber threats continue to plague the digital domain, and the need to improve our defenses continues to grow. Different developers and designers of frameworks have realized that to succeed in this ever-changing landscape, adaptation and flexibility are key to being successful. One of the prominent frameworks, the NIST Cybersecurity Framework 2.0 (CSF 2.0), has endured this changing climate with robust versatility. The CSF was first introduced in 2014, and was re-introduced as the CSF 2.0 in 2024 with additional features like a "Govern" function and updated guidelines to be ever-so effective. This paper will evaluate how effective CSF 2.0 truly is by showcasing how experts view the framework, the policy implications of these views, and how I view the effectiveness and whether CSF 2.0 would be truly successful in this ever-changing digital domain by encapsulating the ethical, political and social aspects of the framework.

Evaluations of CSF 2.0 by Experts

CSF 2.0 is a voluntary framework that includes guidelines and procedures for organizations to follow to maintain their security posture. In terms of effectiveness, there is not a clear-cut approach that solves all issues, as cybersecurity has a multitude of issues with varying difficulty. According to this article by Hossain et al. (2024), a study was conducted to showcase how local entities were conforming their security posture to the CSF 2.0. Researchers were able to conclude that different entities understood the importance of following protocols set forth by the CSF 2.0, but the implantation has been fragmented. The reason for fragmentation was simply due to the challenges set forth like having restraint resources or limited finances that prevented entities, specifically local or smaller groups, from properly aligning their security postures to the CSF 2.0. In conclusion, the research states that the CSF 2.0 ideally would help combat cyber

threats, but its effectiveness would be difficult to determine as its success would be reliant on the incorporation, but the incorporation would be reliant on support from governments and other bigger entities.

In terms of the effectiveness in real world usage, a study was done Bernardo et al. (2025). According to Bernardo et al. (2025), a new methodology was developed to determine the effectiveness of how thorough entities were following the CSF 2.0. To accomplish this, two surveys were conducted, one to investigate how well the entity maintained cybersecurity, and the other was to check on the cybersecurity tools that were being utilized. This study was, in short, a feedback test on how strong security postures were from different entities, as well as ways to improve the CSF 2.0. One thing to note was the flexibility of the CSF 2.0 allowed for organizations to cater to whatever they felt was the most necessary following the CSF 2.0 guidelines of Identify, Protect, Detect, Respond and Recover. In conclusion, experts were able to determine that following frameworks like CSF 2.0 were effective and useful, but ultimately entities should regularly maintain their security posture as well as anticipate and adapt to the ever-changing digital landscape.

The digital landscape and cyber threats are not only exclusive to the United States, but to the entire world. Research conducted by Parmar and Miles (n.d.) presented the differences between the CSF 2.0 and European Union regulated frameworks like the EU Cybersecurity Act. The two had major similarities like the importance of managing risk, regular monitoring and capabilities pertaining to incident responses. However, there are differences that might limit the effectiveness of CSF 2.0. The European Union (EU) have collaborated to create a unified front defending their cyberspace against cyber threats. EU frameworks tend to focus more on regulations and being compliant with the law as opposed to CSF 2.0 being voluntary and

versatile. The differences highlight the effectiveness of CSF 2.0 being limited within the borders of the US as it poses even more challenges for organizations outside the US from catering to the EU framework and CSF 2.0. The study concludes with emphasizing the importance of collaborating with each other, to make the most efficient framework as cyber threats go beyond the borders.

Implications of Policies

The lack of universal implementation suggests the need for CSF 2.0 to have guidelines for all entities, big or small, to properly support and better facilitate the implementation of CSF 2.0 and reduce disparity among the digital domains. Stressing the importance of understanding the need to maintain a regular posture of security and continue adapting to the changing climate to improve not only their own cybersecurity, but the CSF 2.0 with real world usage. Furthermore, understanding the need for cooperation not only among entities in the U.S, but throughout the rest of the world to better incorporate all cybersecurity norms and create a unified front against cyber threats. In conclusion, experts agree that the effectiveness of CSF 2.0 is grand but factors like fragmentation and improper alignment with other nations are truly holding the success of the framework back to reach its full potential and combatting these challenges would have a ripple effect not only on CSF 2.0, but the world and other frameworks that follow suit.

My Assessment

Reviewing studies conducted by experts and researchers, my assessment on the success of CSF 2.0 would rely on how successfully it is implemented, how it is governed, and the international implementation. Measuring how well CSF 2.0 is incorporated in organizations, big or small, and how equal resources are distributed throughout would indicate to me that CSF 2.0

is successful and being properly utilized for its purpose. Measuring how entities improve their cybersecurity posture as opposed to other frameworks, and how seamlessly it's incorporated to the cybersecurity posture. Assessing how the distribution of these postures is managed by those in power, and whether it impacts the cybersecurity norm or culture that entities have created. Assessing the growth or normalization of frameworks, specifically CSF 2.0, not only in the U.S, but the rest of the world, catering to the ever-growing compliances and regulations set forth by different world governments. These are the factors that I would consider when assessing how effective CSF 2.0 is.

Ethical, Political and Social Considerations

Ethically, cybersecurity and proper security posture is a necessity that shouldn't be limited to those with power, money or influence. CSF 2.0's versatility and flexibility allows smaller organizations to implement and acknowledge universal guidelines. However, the disparity between the big and small, rich and poor is present in the digital domain. Politically, with the nature of the framework being voluntary, this showcases the U.S favors private and bigger entities as opposed to smaller and public entities. Socially, everyone deserves to be protected in the digital domain, and the means to protect us, regardless of size or status, should be a universal standard. Being able to access, and having an equal footing is crucial.

Conclusion

In summary, researchers and experts conclude that frameworks like CSF 2.0 are effective and crucial steps in managing cyber threats but are limited by support from the right entities that emphasize encouragement, coordination and global support. My personal analysis on how effective CSF 2.0 is, is based on research and other findings, which is a combination of unified

implementation, proper governance, and worldwide support. If these can be properly incorporated, then I highly believe the CSF 2.0, while already effective, would be able to reach its full potential in effectiveness against cyber threats in the ever-so-changing digital landscape.

References:

Bernardo, L., Malta, S., & Magalhães, J. (2025). An evaluation framework for cybersecurity maturity aligned with the NIST CSF. *Electronics*, *14*(7), 1364. https://doi.org/10.3390/electronics14071364

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Understanding Local Government cybersecurity policy: A concept map and framework. *Information*, *15*(6), 342. https://doi.org/10.3390/info15060342

The NIST Cybersecurity Framework (CSF) 2.0. (n.d.). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Parmar, M., & Miles, A. (n.d.). An assessment between the NIST CSF V2.0 and EU standards. https://indico.esa.int/event/528/attachments/5988/10190/Cyber_Security_Frameworks_SFs_An_Assessment_Between_the_NIST_CSF_v2.0_and_EU_Standards.pdf