IT Security Policy Effectiveness

Samantha Riggs

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Dr. Shideh Yavary Mehr

August 4th, 2025

Perhaps the most valuable factor to consider when analyzing or creating a cybersecurity policy is the overall effectiveness of the policy itself. A strategy that is ineffective or does not meet specific criteria or standards is inevitably not a successful cybersecurity policy. Some policies and regulations may succeed in some manners may fall short of others. “While these regulations have been successful in establishing standards and raising awareness of cyber security, there are still concerns regarding their implementation and enforcement” (Syed, 2019).

Cybersecurity policies, including information technology security policies, can be assessed in a variety of ways. This includes conducting risk assessments, monitoring and analyzing security incidents, audits, compliance checks, and third-party assessments. Kankanhalli et.al. (2003) specifically chose to go along with the audit or compliance check method by utilizing a distributed survey to evaluate information security policy effectiveness after identifying various factors that could contribute to it then subsequently analyzing the collected data. The main route of evaluation appears to be this method of auditing and compliance checks as both Syed (2019) and Chang & Ho (2006) also take a similar approach, by using an empirical survey to evaluated competency and other factors regarding the present policy’s effectiveness.

Assessments regarding information technology and systems security policies in general are considered to be effective policies. This of course depends on whether or not individual policies are properly put into place and are well maintained within an organization. These policies generally provide an outline or guideline for protecting sensitive data, ensuring the security of organization hardware and software, and establishing compliance methods for members of the organization. To ensure that an information technology security policy is currently effective and continues to maintain that effectiveness, regular review, evaluation, and

updates are required. Additionally, measures and mechanisms that ensure enforcement of the policy and organizational policy accountability aid in effectiveness maintenance.

Different factors to consider when creating a cybersecurity policy or strategy in which effectiveness is necessary are ethical concerns, political implications, and social implications. All of these separate considerations are essential to have incorporated within a policy to appropriately address all areas of attention. Any policy that lacks the thorough evaluation of these implications risks not properly addressing all of the needs and requirements that organization cybersecurity demands. Cybersecurity as a whole requires an interdisciplinary approach, meaning that creating a policy cannot rely on a purely technological view. It requires a sociological view, an economic view, a political science view, among many others in order to truly be successful.

References

Ernest Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345–361. https://doi.org/10.1108/02635570610653498

How to evaluate the effectiveness of your cybersecurity strategy. Brandefense. (2024, July 2). https://brandefense.io/blog/drps/how-to-evaluate-the-effectiveness-of-your-cybersecurity-strategy

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of Information Systems Security Effectiveness. *International Journal of Information Management*, *23*(2), 139–154. https://doi.org/10.1016/s0268-4012(02)00105-6

Syed, S. U. "Evaluating the Effectiveness of Cybersecurity Regulations" (2023). *All Student Theses.* 138. https://opus.govst.edu/theses/138/?utm_source=opus.govst.edu%2Ftheses%2F138&utm_medium=PDF&utm_campaign=PDFCoverPages