Atticus Emilsson

CYSE 425W

Cybersecurity Strategy and Policy

April 20, 2025

Policy Analysis 5

Effectivity Assessment Methods for the European Cyber Resilience Act

The EU Cyber Resilience Act (CRA) aims to enhance "cybersecurity standards of products that contain a digital component," and policy highlights a focus on "requiring manufacturers and retailers to ensure cybersecurity throughout the lifecycle of their products" (European Commission, 2024). This paper details a high-level overview of the processes that could be employed to assess the effectiveness of the European Cyber Resilience Act. This process includes the identification and analysis of the policy objectives, methods of implementation, and measures of evaluation.

It is of critical importance that as we progress forward into a digital world, that we properly address pressing aspects of technology such as privacy/security concerns and ethical implications. Considering the abstract nature of applying policies to technology, it is important that researchers sufficiently identify effective methods for evaluating the efficacy of a strategy/policy. The method employed by researchers for the evaluation of policies can vary greatly; however, there are many commonalities which can be observed in the research process. One critical step in many frameworks of evaluation is prior literature review. Literature review

enables researchers to identify/determine the “factors to be measured” and their “measuring methods” (Chaudhary et al., 2022). The identification of such factors is critical to the evaluation of a policy’s performance (Chaudhary et al., 2022). By establishing a solid baseline and control group(s), one can more effectively determine the effectiveness of a policy.

Considering the administrative nature of the policy in question, another complementary route for determining policy effectiveness would be the analysis of compliance-related metrics. This concept can be applied to the CRA by measuring the rate/percentage of organizations that are in-compliance with the policy. This is of course, a more abstract measure; however, it enables investigators to determine the reach in which these new policies have been successfully applied.

Another prominent research approach in evaluating cybersecurity policy effectiveness are surveys. Researchers have effectively leveraged surveys to identify/determine “the most relevant elements,” and factored their importance to derive their “relative weight” (Gafni and Levy, 2023). By applying weight to different factors/facets, researchers can more effectively determine which aspects have a greater effect on one’s cybersecurity posture.

In essence, effectively determining the effectiveness of a cybersecurity policy is a daunting task; however, by successfully integrating different methodologies and approaches, researchers can successfully derive actionable insights as they relate to the plan’s efficacy.

References

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity (Oxford)*, *8*(1). https://doi.org/10.1093/cybsec/tyac006

European Commission. "EU Cyber Resilience Act | Shaping Europe's Digital Future." *Digital-Strategy.ec.europa.eu*, 10 Dec. 2024, digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

Gafni, R., & Levy, Y. (2023). Experts' feedback on the cybersecurity footprint elements: in pursuit of a quantifiable measure of SMBs' cybersecurity posture. *Information and Computer Security*, *31*(5), 601–623. https://doi.org/10.1108/ICS-05-2023-0083