Cybersecurity

J Saintcyr

4/29/2023

Assessing the effectiveness of a cyber security policy

The effectiveness of the cyber security intrusion prevention policy/strategy relates to the measures used to ascertain the effect created in enhancing the quality, security, integrity, and authenticity of data. Assessing the gains that have been made since the implementation of the cyber security intrusion prevention policy is one of the possible ways that can be used to evaluate its effectiveness (Farrand & Carrapico, 2022). A deeper and analytical view into the quality of the stakeholder engagement and involvement subsequent to the process in the formulation and implementation of the policy is a great pointer to its effectiveness. Cultivating the necessary goodwill among the major stakeholders is a critical determinant of the effectiveness of the cybersecurity policy (Sakr et al., 2019). A professional, thorough, and objective audit of the impacts of the cybersecurity policy can paint a clearer picture of its effectiveness. Regular expert opinion on the loopholes in implementation and stakeholder cooperation that need to be sealed can greatly help improve the cybersecurity policy's overall success and impact.

The cognizance of the policy formulators to the fast and ever-changing digital dispensation environment that we are in makes the policy flexible to the changing needs and demands of the market. The aspect of flexibility of the cybersecurity policy is a great determinant of its effectiveness as it illustrates its awareness to react to new and emerging concerns that it had not envisaged when it was being formulated (Sakr et al., 2019). Meeting and operating within the international standards of cybersecurity operations are possible undertakings that an organization with such a policy can use to bolster its effectiveness. Greater standardization and operational coherence from observing certain cybersecurity standards, for instance, the ones applicable to the European Union member states, offer great leverage in making the implementation of the policy effective and successful in meeting its intended objectives (Thomas, 2023). A clear-cut-out analysis of the political, social, and economic implications of the cybersecurity policy on the community are important considerations that must be made in its formulation and implementation. The success of implementing the cybersecurity policy requires all hands on the deck and, more importantly, behavioral change adjustments and new etiquette in how people conduct the affairs in the digital space for data security and integrity to be maintained from the lowest to the highest level.

Enforcing compliance with the cybersecurity policy among the institutions, irrespective of the nature and scope of the work, is an integral component that guarantees its effectiveness and implementation. Measures to address the compliance of the cybersecurity policy despite the inconveniences its causes should be made consistent as they contribute to the desired efficiency of the policy (Farrand & Carrapico, 2022). A compliance clause should be part of the cybersecurity policy as it helps to enhance the conformity of the targeted stakeholders. Regular assessment of the changes that have been witnessed since the cybersecurity policy is an avenue for tracking the progress made progressively in achieving the desired goals and objectives. It is important to note that cybersecurity policy formulation and implementation is a cooperative and collaborative process that requires concerted efforts in wide stakeholder involvement and engagement to make it effective and impactful (Thomas, 2023). Proper communication and coordination in implementing the cybersecurity policy must be seamless as it greatly determines its operational effectiveness.

References

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. European Security, 31(3), 435-453.

Sakr, M. M., Tawfeeq, M. A., & El-Sisi, A. B. (2019). Network intrusion detection system based PSO-SVM for cloud computing. International Journal of Computer Network and Information Security, 11(3), 22.

Thomas, A. J. (2023). Exceeding Authorized Access Under the CFAA. The Open World, Hackbacks and Global Justice, 211–261. https://doi.org/10.1007/978-981-19-8132-6_7