INTERNATIONAL SEVEN JOURNAL
OF MULTIDISCIPLINARY
ISSN: 2764-9547

EVOLVING APPROACHES IN CYBERSECURITY: METRICS AND HUMAN FACTORS

https://doi.org/10.56238/isevmjv1n2-010

Receipt of the originals: 03/11/2022 **Acceptance for publication:** 03/12/2022

Flavio Ambrosio da Silva

ABSTRACT

Recent studies on cybersecurity underscore an increasing recognition of the importance of metrics-driven approaches and adaptable frameworks, particularly for small and medium-sized enterprises (SMEs) that face distinct challenges in a rapidly changing digital landscape. Key developments such as the Cyber Trust Index (CTI) highlight a movement towards methodologies that not only measure security performance quantitatively but also incorporate social and organizational contexts. Additionally, a focus on human factors, including malicious intent, reflects a more nuanced understanding of vulnerabilities within cybersecurity frameworks. The current literature identifies critical gaps in cybersecurity education and workforce development, emphasizing the need for a blend of technical and social skills to foster a culture of responsibility and resilience in organizations. As cybercriminals employ increasingly sophisticated tactics, the integration of advanced technologies, particularly artificial intelligence and cutting-edge cryptographic methods, emerges as a promising avenue for enhancing cybersecurity defenses. In light of the evolving threat landscape, it is essential for organizations and regulators to embrace these innovative practices and frameworks. By adopting effective metrics and remaining adaptable to changing environments, they can bolster their security posture and safeguard critical assets. Ultimately, the establishment of robust metrics and frameworks will facilitate an effective response to cyber threats, paving the way for a more secure future in the digital domain. This strategic shift not only enhances organizational resilience but also contributes to the broader aim of ensuring safety and security in an interconnected world.

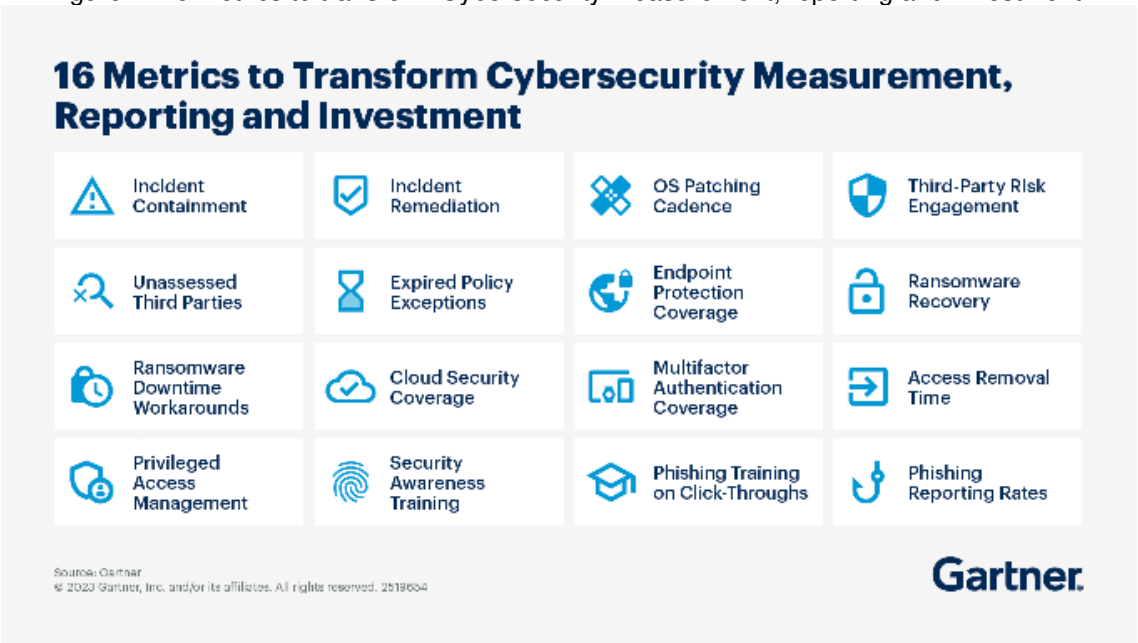
Keywords: Cybersecurity. Metrics. Frameworks. Small and Medium-sized Enterprises (SMEs). Artificial Intelligence.

INTERNATIONAL SEVEN JOURNAL
OF MULTIDISCIPLINARY
ISSN: 2764-9547

INTRODUCTION

The increasing complexity of the cybersecurity landscape, evidenced by the rise of sophisticated threats, makes the adoption of outcome-driven metrics (ODMs) essential for organizations' protection strategies. These metrics are crucial tools that enable stakeholders to clearly observe the relationship between cybersecurity investments and the levels of protection actually achieved. Implementing ODMs provides a quantitative approach to assessing the return on investment (ROI) in cybersecurity, measuring not only the costs of security tools and services but also the practical outcomes of these actions. Indicators such as reduced incident response times, decreased data breaches, and improvements in regulatory compliance demonstrate how investments translate into enhanced protection. Furthermore, outcome-driven metrics facilitate communication among various stakeholders, such as executives, IT teams, and boards of directors, allowing for a clear visualization of the impact of cybersecurity investments, thereby justifying resource allocation. The adoption of ODMs is not just a trend but a strategic necessity for organizations seeking to strengthen their cyber resilience. The ability to clearly demonstrate how cybersecurity investments lead to more robust protection validates the effectiveness of security initiatives and promotes a culture of accountability and proactivity concerning information security.

Figure 1: 16 metrics to transform Cybersecurity measurement, reporting and investment.



Source: Gartner.com (2022).

The study by Haastrecht et al. (2021) addresses the growing challenge faced by small and medium-sized enterprises (SMEs) regarding cyber threats, highlighting the importance of assessing cybersecurity posture as a fundamental step in defending against these risks. SMEs often struggle to navigate the complexities of the current cybersecurity landscape, and risk assessment, often supported by metrics, serves as a basis for adequate defense. However, the study emphasizes that significant challenges still exist, particularly in complex sociotechnical contexts, where seemingly simple issues, such as the aggregation of metrics and the adaptability of solutions, remain under discussion. The researchers analyze these considerations and advocate for integrating metrics into practical frameworks tailored to the specific circumstances and needs of SMEs. To provide valuable insights to researchers and practitioners, the authors developed a new sociotechnical cybersecurity framework aimed at SMEs' needs, revealing an urgent need for intuitive and threat-based approaches to assessing cyber risks, especially for those that are less digitally mature. This framework is expected to help SMEs find more suitable and effective cybersecurity assessment solutions.

The work of Malaivongs, Kiattisin, and Chatjuthamard (2022) highlights that cyber risk is a primary concern that organizations must consider and manage, especially at a time when technology is an integral part of our lives. However, the researchers point to the lack of an efficient and simplified measurement method that organizations or regulators can regularly use to assess and compare the outcomes of implemented cybersecurity efforts, resulting in a critical absence of data for improvements in the field. To address this issue, the study proposes the Cyber Trust Index (CTI), a new simplified framework for assessing, benchmarking, and enhancing organizations' cybersecurity performance. The researchers analyzed relevant scientific articles and widely used security standards to develop foundational security controls that serve as the basis for measurement. The CTI was evaluated by experts and tested in 35 organizations from the critical information infrastructure (CII) sector and other sectors in Thailand, confirming its validity and reliability in real-world scenarios. The results revealed that the CTI consists of basic controls and ranking methods, covering 12 dimensions, 25 clusters, and 70 controls, and emphasizes the importance of internal and external factors influencing cybersecurity performance. The study concludes that the CTI is a valid and effective tool for measuring cybersecurity performance, offering a roadmap for

organizations and regulators to adopt and adapt this framework in their measurement and improvement initiatives.

The study by King et al. (2018) investigates the growing impact of cyberattacks on networks, systems, and users, emphasizing the need for enhanced methods to predict vulnerabilities in systems. The researchers highlight the importance of characterizing the human factors that contribute to vulnerabilities and cybersecurity risks, focusing on the roles of rationality, experience, and malice. Despite the significant impact of malice on cyber risk, literature on this human characteristic is scarce. To fill this gap, the Collaborative Cybersecurity Research Alliance (CSec-CRA) developed a human factors risk framework that describes the characteristics of attackers, users, and defenders, all capable of influencing cyber risk. The study discusses the existing literature on malice and proposes assessment metrics within the context of the framework. It defines malice as the intent to cause harm and critiques current research that mainly focuses on detecting malicious software, often neglecting the analysis of individual intent behind cyberattacks. By exploring human malice through observable behaviors and social interactions, the researchers aim to develop analyzable metrics to better understand and assess the risks posed by individuals in the cyber domain. The article has dual objectives: to review the relevant literature across various disciplines and to identify initial assessment metrics to characterize human malice in cybersecurity, integrating these metrics into comprehensive risk analyses.

The study by Slapničar et al. (2020) aims to evaluate the effectiveness of internal cybersecurity audits by developing a Cybersecurity Audit Index encompassing three dimensions: planning, execution, and reporting. The researchers hypothesized that the effectiveness of cybersecurity audits is positively correlated with the maturity of cyber risk management and negatively correlated with the likelihood of successful cyberattacks. Through a survey of auditors and Audit Directors from various countries and industries, they discovered that Cybersecurity Audit Index scores varied significantly, averaging 58 on a scale of 0 to 100. While a strong positive correlation was found between the planning and execution dimensions, the relationship with the effectiveness of reporting to the Board was weaker. Consistent with the hypothesis, the Cybersecurity Audit Index was positively associated with cyber risk maturity; however, contrary to expectations, it showed no correlation with the probability of a cyberattack.

This research represents the first comprehensive measurement of the effectiveness of cybersecurity audits and their implications for cyber risk management.

Finally, the study by Dawson and Thomson (2018) addresses the challenges in assessing the current state of cybersecurity education and workforce development, highlighting the lack of quantitative assessments regarding the cognitive skills, job roles, and team dynamics essential for cybersecurity professionals to succeed. The authors argue that success in the cyber domain requires a combination of technical skills, domain-specific knowledge, and social intelligence. They emphasize that cybersecurity professionals must also incorporate characteristics such as reliability, integrity, and resilience, complicating the definition of the necessary skills, knowledge, and attributes beyond mere technical training. Existing research predominantly focuses on technical and engineering skills, often neglecting significant social and organizational factors that influence success in real-world scenarios. Throughout the review, Dawson and Thomson identify gaps in the literature on cybersecurity specialization and workforce development, advocating for the importance of recognizing social suitability within the diverse cybersecurity workforce. They outline six key assumptions for the future development of the cybersecurity workforce, including the need for systems thinkers, team players, commitment to continuous learning, strong communication skills, a sense of civic responsibility, and a combination of technical and social skills. The article concludes with recommendations for developing social and cognitive metrics that could serve as indicators of future performance in cybersecurity-related roles, offering a roadmap for future research in the field.

The study conducted by Zeadally et al. (2020) investigates the accelerated evolution of the cybersecurity field, which has consistently appeared in the news due to the rise in threats and the ongoing efforts of cybercriminals to outpace law enforcement. While the underlying motives for cyberattacks remain largely consistent, the sophistication of the techniques employed by cybercriminals has increased, rendering traditional cybersecurity solutions inadequate for detecting and mitigating new threats. The authors highlight the potential of innovations in cryptographic methods and Artificial Intelligence (AI), particularly in machine learning and deep learning, as promising pathways for cybersecurity experts to combat the ever-evolving challenges presented by adversaries.

The analysis of recent studies on cybersecurity reveals a growing awareness of the need for metrics-driven approaches and adaptable frameworks, especially for small and medium-sized enterprises (SMEs) facing unique challenges in this ever-evolving environment. The development of indices like the Cyber Trust Index (CTI) and the emphasis on human factors, such as malice, indicate a shift toward methodologies that not only quantify security performance but also consider the social and organizational context. The gaps in cybersecurity education and workforce development highlight the urgency of integrating technical and social skills, fostering a culture of responsibility and resilience. As cybercriminals become more sophisticated, the application of new technologies, such as artificial intelligence and advanced cryptography, shows promise for enhancing cybersecurity defenses. Therefore, it is imperative that organizations and regulators adopt these innovative practices and frameworks to strengthen their security posture and protect critical assets in an increasingly threatening digital landscape. The implementation of effective metrics and adaptation to a dynamic environment are not only necessary but essential to ensure an effective response to cyber threats and promote a safer future in the digital domain.

REFERENCES

1. Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology, 9*, 744. https://doi.org/10.3389/fpsyg.2018.00744

2. Haastrecht, M., Ozkan, B., Brinkhuis, M., & Spruit, M. (2021). Respite for SMEs: A systematic review of socio-technical cybersecurity metrics. *Applied Sciences, 11*(15), 6909. https://doi.org/10.3390/app11156909

3. King, Z., Henshel, D., Flora, L., Cains, M., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in Psychology, 9*. https://doi.org/10.3389/fpsyg.2018.00039

4. Malaivongs, S., Kiattisin, S., & Chatjuthamard, P. (2022). Cyber trust index: A framework for rating and improving cybersecurity performance. *Applied Sciences, 12*(21), 11174. https://doi.org/10.3390/app122111174

5. Slapničar, S., Vuko, T., Cular, M., & Drascek, M. (2020). Effectiveness of cybersecurity audit. *Corporate Finance: Governance.* https://doi.org/10.2139/ssrn.3741877

6. Zeadally, S., Adi, E., Baig, Z., & Khan, I. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access, 8*, 23817-23837. https://doi.org/10.1109/ACCESS.2020.2968045