Evolving Approaches in Cybersecurity: Metrics and Human Factors

FLAVIO AMBROSIO DA SILVA[1], ELIOMAR GOTARDI PESSOA[2], HUGO SANTOS[3], WILSON LEITE REBOUÇAS FILHO[4], LEONARDO DA SILVA[5], CARLOS EDUARDO CAMPOS DE OLIVEIRA[6], LUIS JOIVAN NUNES DAHMER[7]

[1, 2, 3, 4, 5, 6, 7] *Pontifícia UniversidadeCatólica do Rio Grande do Sul (2020)*

Abstract- The increasing complexity of cybersecurity threats demands new approaches to enhance digital security, particularly for small and medium-sized enterprises (SMEs), which face unique challenges in adapting to a rapidly evolving technological landscape. This study explores the role of metrics-driven cybersecurity frameworks and the importance of integrating human factors into security models. It highlights the significance of the Cyber Trust Index (CTI) as an innovative methodology that combines quantitative security performance assessment with organizational and social contexts. Additionally, the research underscores the growing need for cybersecurity education and workforce development, emphasizing the integration of artificial intelligence (AI) and advanced cryptographic techniques as key components in fortifying digital infrastructures. The findings suggest that the adoption of flexible cybersecurity frameworks and advanced threat detection models is essential for organizations to enhance resilience and maintain robust security measures. The paper concludes by discussing the implications of these frameworks for future cybersecurity policies and industry best practices.

Indexed Terms- Cybersecurity, Metrics, Artificial Intelligence, Cyber Trust Index, SMEs, Cryptographic Methods

I. INTRODUCTION

The expansion of cyber threats has led organizations to rethink security strategies, shifting towards metrics-driven and adaptive cybersecurity models. The increasing reliance on AI-driven cybersecurity solutions has raised new challenges, particularly regarding the need for a human-centered approach that balances technology with behavioral cybersecurity factors. This study explores how organizations can integrate security metrics and human factors to build resilient cyber defenses, particularly for SMEs that often lack the resources of larger corporations.

Metrics are fundamental for understanding cybersecurity effectiveness and optimizing defense strategies. Traditional cybersecurity models have often focused on technical measures, but recent trends indicate that a combination of organizational, technical, and behavioral metrics offers a more comprehensive evaluation of cyber risks. One of the emerging methodologies is the Cyber Trust Index (CTI), which provides an assessment framework that integrates social and organizational factors alongside technical security metrics. This innovative model allows companies to evaluate their security posture not only in terms of system vulnerabilities and risk detection but also based on employee behavior, organizational resilience, and response readiness.

AI has significantly transformed cybersecurity, enabling predictive analytics, anomaly detection, and automated threat response. The integration of machine learning algorithms and deep learning models has improved security frameworks by allowing real-time analysis of cyber threats and behavioral patterns. However, despite these advancements, human factors remain a critical aspect of cybersecurity strategy. AI-driven security tools can identify malicious activity patterns and automate incident response, but the human decision-making process is essential in interpreting security alerts and mitigating false positives. Organizations must therefore focus on training cybersecurity professionals to work alongside AI systems, ensuring a balanced approach that leverages technology without overlooking human expertise.

Cybersecurity is not only about technology—it is also about human behavior. Studies have shown that a large percentage of cyber incidents result from human error, social engineering attacks, and lack of security awareness. Organizations that fail to address the human aspect of cybersecurity remain vulnerable, regardless of their technological investments. To mitigate these risks, cybersecurity frameworks must incorporate training programs that educate employees on phishing attacks, social engineering, and security hygiene, behavioral analytics to monitor and predict potential insider threats and human-driven vulnerabilities, and adaptive security policies that account for organizational culture and employee cybersecurity engagement. The integration of human factors into cybersecurity strategies enhances the effectiveness of security frameworks, leading to better risk assessment and threat mitigation.

SMEs often lack the financial and technological resources available to large enterprises, making them prime targets for cyberattacks. The adoption of cost-effective cybersecurity solutions, such as metrics-based frameworks and AI-driven defenses, can help bridge this gap. However, government agencies and industry leaders must also play a role in developing policies that support SMEs in implementing affordable and scalable cybersecurity solutions. Looking ahead, the future of cybersecurity will depend on the ability of organizations to adopt dynamic and flexible cybersecurity metrics to measure real-time threats, integrate AI and automation while maintaining human oversight in security decisions, develop stronger cybersecurity awareness programs for employees, and collaborate across industries to share threat intelligence and improve security postures collectively. By prioritizing these strategies, organizations can enhance their cybersecurity resilience and protect critical assets from emerging digital threats.

As cyber threats continue to evolve, so must cybersecurity frameworks. The combination of quantifiable security metrics, AI-driven solutions, and human-centric approaches represents the future of effective cyber defense strategies. Organizations that embrace adaptive security models will be better equipped to handle emerging threats while fostering a culture of cybersecurity awareness and innovation. By investing in education, AI technology, and human-centered cybersecurity policies, businesses can create a sustainable cybersecurity ecosystem that is both proactive and resilient.

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] 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