**Report on Cyber Threat Visibility Challenges for SMEs and Developing Economies**

**Abstract**

This study is based on exploring the obstacles encountered by Small and Medium-sized Enterprises (SMEs) and emerging economies in upholding visibility over cyber threats, with the aim of gaining insight into their specific cybersecurity requirements and difficulties. It mentions various reasons along with evident studies that showcases the lack of cyber security awareness among SMEs and Developing Economies. At the same time, however, entrepreneurs are often unprepared for cybersecurity needs, the policymakers, industry, and nonprofit groups that support them also face technological and knowledge constraints in keeping up with their needs. This research comprises of some of the major challenges faced by SMEs that are responsible for the lack of their cyber security.

Keywords: Cybersecurity, SMEs, Developing Economies, Cyber Threat Visibility.

**Table of Contents-**

Abstract…………………………………………………………………………………………….1

Table of Contents………………………………………………………………………………1

Introduction………………………………………………………………………………………2

Methodology…………………………………………………………………………………… 2

Overview…………………………………………………………………………………………..2

Challenges………………………………………………………………………………3

Strategies……………………………………………………………………………….4

Conclusion…………………………………………………………………………………………4

References…………………………………………………………………………………………5

**Introduction**

Small and Medium Enterprises (SMEs) and developing economies face significant challenges in maintaining cyber threat visibility, leading to vulnerabilities and cybersecurity risks. While cyberattacks have become a major concern for businesses globally, SMEs and developing economies face a unique challenge in maintaining cyber threat visibility due to limited resources and a lack of cybersecurity awareness. This report aims to analyze the reasons behind the inability of SMEs and developing economies to maintain cyber threat visibility and understand their cybersecurity needs and challenges.

**Methodology**

The research utilizes an extensive review of existing evidence to investigate the obstacles encountered by Small and Medium-sized Enterprises (SMEs) and emerging economies in sustaining visibility of cyber threats. The report focuses on some of the necessary reasons that are accountable for the challenges. It also depicts various limitations faced by SMEs and developing economies, such as limited resources, lack of skilled force, inadequate awareness, and limited access to latest technologies. (Saeed et al., 2023)

The methodology also suggests some ways to identifying and solve the existing challenges encountered by SMEs and developing economies.

**Overview**

SMEs are not well prepared to defend themselves from cyber threats and attacks, and some of them can't even detect data breaches and manage cyber security risks. Employee behaviour in SMEs could account for many cybersecurity threats. For instance, ignoring information policies, organizational guidelines, and company rules leads to many cybersecurity threats. consistent concern in literature has been the lack of seriousness in SMEs’ usual ways of dealing with cybersecurity threats. Many SMEs have not prioritized cybersecurity guidelines or taken proactive measures to address potential threats, exacerbating their vulnerability to cyberattacks. SMEs encounter numerous challenges when it comes to cybersecurity. Despite recognizing cyber threats as a top concern, nearly half cite insufficient budget as the primary barrier to implementing effective cybersecurity measures. This financial limitation frequently exposes SMEs to cyber-attacks, as they find themselves lacking the necessary resources and knowledge to effectively safeguard against, deter, or identify such threats. Below mentioned are some of the major challenges explained briefly that SMEs faced and proved to be responsible for the lack of cybersecurity among SMEs and Developing Economies. (Saha and Anwar, 2024)

**Challenges Faced by SMEs**

1. Limited Resources and Budget Constraints

SMEs and developing economies often operate with limited resources and face budget constraints, which hinders their ability to invest in robust cybersecurity measures. Due to competing priorities, cybersecurity initiatives may receive inadequate funding, leading to insufficient tools, technologies, and personnel to maintain cyber threat visibility effectively.

2. Lack of Skilled Workforce

Many SMEs and developing economies struggle with a shortage of skilled cybersecurity professionals. Without personnel with the necessary expertise, organizations find it challenging to implement and manage cybersecurity solutions effectively. This shortage exacerbates the difficulty of maintaining cyber threat visibility, as there are insufficient resources to monitor, detect, and respond to evolving threats.

3. Limited Access to Advanced Technologies

Access to advanced cybersecurity technologies is often limited for SMEs and organizations in developing economies. These technologies, such as threat intelligence platforms, advanced analytics, and machine learning algorithms, play a crucial role in identifying and mitigating cyber threats. However, due to cost barriers and technological dependencies, many SMEs and developing economies rely on basic security tools, which offer limited visibility into sophisticated cyber threats. (Saeed et al., 2023)

4. Inadequate Cybersecurity Awareness and Education

A lack of cybersecurity awareness and education among employees and decision-makers contributes to the challenge of maintaining cyber threat visibility. Without a solid understanding of cybersecurity best practices, individuals may engage in risky behaviours, such as clicking on suspicious links or neglecting security protocols, inadvertently exposing organizations to cyber threats. Furthermore, limited awareness among leadership may result in underinvestment in cybersecurity initiatives.

SMEs require personnel with expertise in cybersecurity training and the ability to effectively educate others to enhance awareness and provide support for employee cybersecurity training initiatives. According to a survey conducted for the same, only 45 out of 141 SMEs have positions dedicated to cybersecurity and that only 27 out of 141 SMEs provide cybersecurity training. Thus, 18 out of 141 SMEs that have positions dedicated to cybersecurity do not offer cybersecurity training.

5. Cross-Sectoral Cyber Risks

SMEs and organizations in developing economies often participate in interconnected supply chains and business ecosystems. Cyber risks in one sector can propagate across the supply chain, affecting multiple organizations. Limited visibility into the cybersecurity posture of partner organizations increases the likelihood of cyber threats spreading unchecked, posing significant challenges for maintaining cyber threat visibility. (Erdogan et al., 2023)

**Strategies for the above Challenges-**

1. Employee training and awareness programs-

It is essential to have continuous training programs to keep employees informed about evolving cyber threats. The kind of awareness campaigns you should have need to cover the basics of recognising a potential cyber-attack and the importance of reporting any security incidents promptly. (www.interscale.com.au, n.d.)

2. Regular system audits and updates-

To identify and rectify potential security incidents, it is necessary to have routine audits of systems and software. This would also help to improve the technology and software used by SMEs and make sure that they are using the updated software versions. (www.interscale.com.au, n.d.)

3. Policy and Regulatory Support-

Establish policies that promote and facilitate the adoption of cybersecurity practices among SMEs. This may involve providing incentives to encourage investments in cybersecurity, outlining minimum standards for cybersecurity, and offering assistance for cybersecurity training initiatives.

**Conclusion-**

Maintaining cyber threat visibility is critical for SMEs and developing economies to mitigate cybersecurity risks effectively. However, various challenges, including limited resources, a shortage of skilled personnel, inadequate technologies, and low cybersecurity awareness, hinder their ability to achieve this goal. Addressing these challenges requires collaborative efforts from governments, industry stakeholders, and cybersecurity professionals to provide support, resources, and education necessary to enhance cyber threat visibility and strengthen cybersecurity resilience in SMEs and developing economies. By understanding the challenges faced by businesses and addressing them through a comprehensive policy framework, they can hope to empower small business owners, to build more secure and successful businesses.

**References-**

1. www.interscale.com.au. (n.d.). Solving Common Cybersecurity Issues In Small To Medium Enterprises | Interscale. [online] Available at: https://www.interscale.com.au/blog/solving-common-cybersecurity-issues-in-small-to-medium-enterprises [Accessed 2 Apr. 2024].

2. Saha, B. and Anwar, Z. (2024). A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework. Journal of Information Security, [online] 15(01), pp.24–39. doi:https://doi.org/10.4236/jis.2024.151003.

3. Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S. and Pickering, J. (2023). Cybersecurity Awareness and Capacities of SMEs. Proceedings of the 9th International Conference on Information Systems Security and Privacy. doi: https://doi.org/10.5220/0011609600003405.

4. Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E. and Alabbad, D.A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, [online] 23(15). doi: https://doi.org/10.3390/s23156666.