Assessing SMEs' and Developing Economies' Cyber Threat Visibility Challenges

Abstract:

SMEs and emerging economies confront distinct problems in maintaining cyber threat visibility owing to a variety of issues such as limited resources, a lack of knowledge, poor infrastructure, and a dynamic cyber threat environment. While large companies may have specialised cybersecurity teams and advanced systems for monitoring and detecting cyber threats, small and medium-sized businesses frequently lack such skills. Similarly, underdeveloped economies may have less financing for cybersecurity activities and may place a higher priority on other developmental goals.

Introduction:

Cybersecurity is crucial in today's digital environment for all businesses, but it's especially important for Small and Medium-Sized Enterprises (SMEs) and those operating in developing nations. Nevertheless, these organisations often struggle with issues like few resources, insufficient knowledge, and low awareness, which makes it difficult for them to keep an eye on cyber threats and implement efficient cybersecurity solutions. They thereby run a higher risk of losing money, damaging their brand, and facing legal ramifications due to the confidentiality, integrity, and availability of their digital assets. In order to create customised solutions and support systems that will increase SMEs' and organisations' cyber resilience, it is crucial to comprehend the unique issues that these businesses confront in emerging countries. Stakeholders can enable SMEs and emerging economies to effectively protect their digital infrastructure and successfully negotiate the complicated cybersecurity landscape by tackling these obstacles head-on.

Current Trends:

SMEs and organisations in emerging countries now face greater cybersecurity risks as a result of the quickly evolving digital landscape, rising business connectivity, and increasingly sophisticated cyberthreats. Some key trends include:

- **Ecosystem Vulnerability:** Due to the increased attack surface created by the interconnection of firms within digital ecosystems, SMEs and developing economy organisations are more susceptible to supply chain and third-party assaults.

- **Resource Constraints:** Compared to bigger businesses, SMEs and organisations in developing nations frequently lack the financial, technological, and human resources to invest in effective cybersecurity solutions.

- **Lack of Knowledge and Experience**: Many SME owners, managers, and staff lack knowledge and experience in cybersecurity, which makes it difficult for them to recognise and counteract cyber risks. This deficiency extends to organisations operating in emerging economies.

- **Evolving Threat Landscape**:SMEs and emerging economy organisations are unable to keep up with the required security upgrades and procedures due to the fast growth of cyber threats including ransomware, phishing, and advanced persistent attacks.

Cybersecurity Challenges for SMEs and Developing Economies

SMEs are the backbone of the economy and a major contributor to GDP and jobs in many developing nations. They frequently lack the tools and knowledge necessary to properly handle cybersecurity threats, though. These nations' governments and regulatory agencies are realising more and more how crucial it is to assist SMEs in raising their visibility to cyber threats.

1) *Limited Resources and Budget Constraints*: Financing constraints and resource scarcity frequently prevent SMEs and organisations in emerging nations from investing in comprehensive cybersecurity solutions. Their ability to purchase cutting-edge security solutions, employ qualified cybersecurity experts, and put in place thorough security procedures is hampered as a result.[1] [2]
2) *Lack of Cybersecurity Expertise:* It is challenging for many SMEs and emerging economy organisations to detect vulnerabilities, create efficient security plans, and handle cyber events as they lack internal cybersecurity competence. According to a World Economic Forum poll, 48% of SMEs in developing nations cited a major difficulty as a lack of cybersecurity expertise.
3) *Inadequate Security Awareness and Training*: Employees at SMEs and in developing economies often lack proper security awareness and training, leaving them vulnerable to common threats like phishing and social engineering attacks. A study by the National Cyber Security Centre in the UK found that 83% of SMEs reported employee mistakes as a contributing factor to security breaches.[1]
4) *Evolving Threat Landscape*: Business email compromise (BEC) assaults and ransomware are two examples of cyberthreats that are evolving faster in SMEs and emerging economy organisations can keep up with the required security upgrades and procedures. According to World Economic Forum research, 40% of SMEs in developing nations had a cybersecurity issue during the previous year.[2][4]
5) *Ecosystem Vulnerability:* SMEs and emerging economy organisations are particularly susceptible to compromise through supply chain and third-party attacks due to the increased attack surface caused by the interconnection of firms within digital ecosystems. The cybersecurity of their supply chain partners worried 74% of SMEs in the EU, according to a research conducted by the European Union Agency for Cybersecurity (ENISA).[4]

6) *Regulatory and Policy Gaps:* SMEs in developing economies may lack clear direction and assistance in enhancing their cyber resilience due to inadequate or inadequately implemented cybersecurity laws and policies. According to a National Cybersecurity Authority survey conducted in Saudi Arabia, 62% of the nation's non-governmental organisations were ignorant of relating cybersecurity laws.[3]

7) *Inadequate Infrastructure:* SMEs frequently use antiquated software and IT infrastructure, making them more vulnerable to cyberattacks. Furthermore, cybersecurity vulnerabilities are made worse by the absence of frequent updates and fixes.[5]

Tackling the Challenges:

A multifaceted strategy is needed to solve the issues with cyber threat visibility that SMEs and organisations in emerging economies face.

Enhancing Cybersecurity Awareness:

- In industrialised nations such as the UK, governments, industry groups, and cybersecurity specialists have worked together to create and execute focused awareness campaigns and training initiatives aimed at enlightening SME owners, managers, and staff members about cyber hazards and recommended practices.

- Initiatives like Monsha'at and the National Cybersecurity Authority (NCA) are attempting to increase cybersecurity awareness among SMEs in emerging nations like Saudi Arabia. [1]

Providing Accessible Cybersecurity Solutions:

- In developed nations, governments and tech companies are collaborating to create and advertise reasonably priced, easily navigable cybersecurity products and services that are suited to small and medium-sized enterprises' requirements.
- It is necessary to increase the accessibility and availability of these cybersecurity solutions for SMEs in developing economies.[3]

Strengthening Regulatory and Policy Frameworks:

- To give SMEs a clear framework for enhancing their cyber resilience, policymakers in industrialised nations such as the UK have put in place strict cybersecurity rules, guidelines, and support systems.[1]
- Though further development is certainly required, developing nations like Saudi Arabia are likewise striving to improve their cybersecurity legislative and administrative frameworks to better assist SMEs.

Fostering Ecosystem Collaboration:

- Developed countries are encouraging information sharing, threat intelligence exchange, and collaborative security initiatives within digital ecosystems to help SMEs collectively enhance their cyber threat visibility and resilience.
- Developing economies could benefit from similar ecosystem-level collaboration efforts to support SMEs in addressing cybersecurity challenges.

Leveraging Emerging Technologies:

- In order to assist SMEs in overcoming their resource limitations and strengthening their cybersecurity posture, developed nations are encouraging the use of cutting-edge solutions like managed security providers, cloud-based security services, and AI-powered threat detection.
- The strategic application of these new technologies to improve the cyber resilience of SMEs might also be investigated by developing countries, however adoption might be slower because of infrastructure and resource constraints.

Few Proposed Solutions:

Cybersecurity Education and Training:

Awareness Campaigns:
Use webinars, seminars, and online resources to conduct focused campaigns that inform SMEs about cybersecurity best practices and dangers. For efficient outreach, cooperate with governmental organisations and trade groups.

Training Programmes: Provide thorough training courses on a range of cybersecurity-related subjects, with online and in-person options. Using certificates to attest to completion will encourage the development of skills.

Access to Affordable Tools and Resources:

Subsidised Solutions: Work with partners in the business and government agencies to offer grants or discounts on cybersecurity equipment. Investigate subscription methods to provide SMEs with access to solutions.

Open-Source Solutions: Encourage the adoption of affordable open-source software for strong security features. Promote involvement in open-source groups to facilitate knowledge exchange and assistance.

Government Assistance:

Financial Incentives: To entice SMEs to invest in cybersecurity, provide grants, tax exemptions, or loans. Create financing initiatives specifically for SMEs and help them take advantage of these possibilities.[4]
Regulatory Support: Offer direction and assistance to ensure adherence to cybersecurity laws. Provide streamlined frameworks and instructional materials to help SMEs comply with regulations.

Conclusion:

In conclusion, emerging economies' Small and Medium Enterprises (SMEs) must adopt a multifaceted strategy to improve cybersecurity resilience. SME resilience against cyber threats may be greatly enhanced by emphasising cybersecurity education and training, granting access to reasonably priced technologies and resources, and giving financial incentives and regulatory support from the government. Effective implementation requires cooperation amongst stakeholders, which includes SMEs, governments, trade groups, and cybersecurity specialists. SMEs can strengthen the security of their digital assets and help emerging economies create a more secure digital environment by working together to address these issues.

References :

[1]Rawindaran, N. *et al.* (2023) *Enhancing cyber security governance and policy for smes in industry 5.0: A comparative study between Saudi Arabia and the United Kingdom, MDPI*. Available at: https://www.mdpi.com/2673-6470/3/3/14 (Accessed: 05 April 2024).

[2]*State of Technology at UK smes*. Available at: https://www.ogl.co.uk/ckfiles/OGL_State_of_Technology_Research_Report_2020.pdf?dm_i=1J5D%2C6ORST%2C5Z9OPC%2CQOF3J%2C1 (Accessed: 05 April 2024).

[3]Global Cybersecurity Outlook 2022 | weforum. Available at: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

[4] Cybersecurity Guide for smes - 12 steps to securing your business (2022) *ENISA*. Available at: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes (Accessed: 05 April 2024).

[5]Team, S.T. (2023) *Best cybersecurity solutions for small businesses in 2023*, *Security Tools*. Available at: https://www.security-tools.com/best-cybersecurity-solutions-for-smbs-in-2023/ (Accessed: 05 April 2024).