Assessing SMEs' and developing economies' cyber threat visibility challenges

Abstract

SMEs are vital for economic growth, but they are vulnerable to cyberattacks. SME owners need to recognise the potential impact of a cyberattack and take measures to protect their businesses. This report categorises the challenges that SMEs face based on global economic and cybersecurity challenges. SMEs need help creating policies and complying with regulations to prevent financial losses from cybersecurity risks. SMEs must adopt quantitative research approaches to address this issue. Good cybersecurity strategies include identifying assets and risks, protecting accounts and data, implementing a continuity plan and monitoring and reviewing.

Keywords: SMEs, cybersecurity, challenges, frameworks, economy

Table of Contents

Introduction

Small and medium-sized enterprises (SMEs) are essential for the global economy since they play a crucial role in sustainable economic growth. It is vital to make cyber security strategies to

improve the economy's welfare in SMEs. They are particularly vulnerable to cyberattacks, which can have so many consequences. Cybercrime is increasing in frequency and impact, making SMEs a likely target. They often have valuable data and a network breach can grant access to larger corporate networks. They also possess resources that make them more attractive to cybercriminals than individual users. Unfortunately, SMEs often lack cybersecurity awareness and budget. They may prioritise other regulatory burdens over cybersecurity [3]. When a cyberattack occurs, it can lead to severe financial losses, as well as damage to a company's reputation, pricing structure and productivity. Therefore, it is essential for SME owners to recognise the potential impact of a cyberattack and take measures to protect their businesses.

These vulnerabilities increase the risk of undetected threats, limit the ability to fix issues in a timely manner and increase potential damages. SMEs also rely heavily on networked devices and software services, making them vulnerable to business interruption and potentially threatening their livelihood [3].

The main aim of this report is to provide the challenges that SMEs have faced based on the articles I've researched, which will be helpful in providing cybersecurity strategies with minimal cost. This article also explains overall challenges that have been categorised based on global challenges faced in economy and cybersecurity.

Methodology

Article 1 studies how global challenges in economic competition impact SMEs. 110 out of 256 journal papers were selected. It aims to understand the challenges and strategies adopted by SMEs [1].

Article 2 reports that most SMB cyber security researchers used qualitative methods (70%) to assess cyber risk, while the remaining used quantitative methods. Literature reviews, surveys and interviews were the most common data collection methods [2].

Challenges

The challenges I've researched in both articles are a mix of global and cybersecurity categories.

Global economic competition has intensified due to globalization and the WTO trade regime which has negatively impacted SMEs, particularly those in the textile and clothing industry. SMEs face challenges in implementing innovations due to inadequate budgets,

lack of resources and difficulties in expanding existing capacity. The government can assist SMEs in improving innovation and technology adaptations, which is essential for SMEs to be competitive globally [1]. The global economic crisis is caused by trade imbalances, US consumption patterns, capital market deregulation and the dominance of the US dollar. SMEs in the automotive industry are heavily impacted, but they are more adaptable and flexible than large businesses. Governments can implement supportive policies to aid the recovery process [1].

SMEs often overlook cybersecurity risks, assuming that limiting their online presence can protect them. However, cyber threats extend beyond websites and social media and can affect any internet-connected device. This can lead to significant financial losses and disruptions to their business, industry, or supply chain [2]. SMEs are vulnerable to cyber-attacks due to a lack of awareness and knowledge about cybersecurity. They need help with creating policies and complying with regulations [2].

ICT has enabled SMEs to go global. The internet is crucial for knowledge transfer. SMEs can save resources by embracing the internet. Soft infrastructure, such as full internet access and cheap web hosting, expands sales and presentations. E-commerce and m-commerce benefit SMEs. Social networks play a vital role in entrepreneurship. Cybersecurity is a significant challenge [1]. Crowdfunding is an additional way of gathering funds [1]. MNCs dominate the global market, posing a challenge to SMEs in developing nations. Collaborating with MNCs can help SMEs eradicate resource shortcomings and benefit from access to export markets and productivity gains. However, local ventures should not rely solely on MNCs to prevent monopolistic industry frames [1]. TNCs impact host country economies by sourcing locally and using territorial networks for production. Local SMEs act as TNC suppliers by providing parts, components and manufacturing services. Local suppliers have valuable knowledge embedded in regional links, technical specifications, standards and management patterns, often providing assistance to TNCs. There's even evidence of reverse transmission of technological knowledge from SMEs to TNCs [1].

SMEs have limited resources for dealing with cyberattacks and face challenges in adopting advanced cybersecurity technologies due to high costs. They often rely on IT service providers for cybersecurity but lack necessary contractual arrangements. Therefore, affordable, easy-to-implement cybersecurity solutions are required [2]. SMEs struggle with cybersecurity as threats evolve faster than technology. Inexperience with security tech and third-party risks leave them ill-prepared to deal with IoT risks [2].

SMEs struggle to find help when responding to cybercrime events. Multiple sources of information often cause confusion. Reframing how we think about cybersecurity can help businesses gain credibility and drive growth [2]. SMEs care about cybersecurity, but can become lax over time. They are inconsistent in implementing security measures based on their risk assessment. Cybersecurity initiatives can be challenging for small businesses to quickly respond to emerging threats [2].

Discussion

SMEs face a range of challenges in their quest for survival, including intense competition, limited resources and evolving customer demands. To overcome these hurdles, they often adopt various strategies such as cost leadership, SWOT and PESTEL analyses, maximising internal resources and educational programs to stay ahead in the game [1]. However, to gain a sustainable competitive advantage, SMEs must identify the right product with comparative advantages [1].

One of the most critical challenges that SMEs face today is cybersecurity. Unfortunately, the field of SME cybersecurity lacks original research, particularly in local contexts. While qualitative methods can be quick and cost-effective, empirical research is necessary to understand the issues and provide better solutions [2]. With cyber-attacks becoming more sophisticated, SMEs must not only defend against them but also return to normal operations after an incident. Therefore, good cybersecurity strategies are crucial to their success. These strategies include identifying assets and risks, protecting accounts and data, implementing a continuity plan and monitoring and reviewing. However, it is often challenging for SMEs to practically implement these practices, which is why NIST and Secure Control frameworks have been proposed for their implementation order [2].

SMEs often lack resources for proper cybersecurity, making them an easy target for cybercriminals. They may not have the financial means or incentive to invest in protection, which could result in negative spill-over effects [3]. As a result, it's important to analyze the challenges they face in implementing cybersecurity measures, given their importance for innovation, employment and economic growth [3].

Conclusion

Cybersecurity plays an essential role in the development of effective solutions for the needs of SMEs.

It indicates some considerable effort has been made to develop security strategies and policies for SMEs, but there has been limited work due to practical implementation, detection, response and recovery. With deeper analysis of how SMEs implement security controls, they should adopt well-established quantitative research approaches to address this issue in future studies.

Framework such as NIST and CS shows that they are primarily focused on information security policies and operational security [2]. There is a significant gap in research on cyber security incidents. Hence, the main focus should be towards cyber resilience to ensure a balanced approach to cyber prevention, response and recovery.

While cyber-attacks are inevitable, SMEs must be equipped to respond and recover from such incidents. Some rules require SMEs to have good cybersecurity. However, these rules are complex and can be hard to follow [3]. Even if businesses know about the risks, they might not know how to protect themselves. The rules can be really difficult to understand, especially if the business is small and doesn't have many employees. They might not have much experience with cybersecurity and have other things to worry about [3].

References

[1] Naradda Gamage SK, Ekanayake E, Abeyrathne G, Prasanna R, Jayasundara J, Rajapakshe P. A Review of Global Challenges and Survival Strategies of Small and Medium Enterprises (SMEs). Economies. 2020; 8(4):79. https://doi.org/10.3390/economies8040079

[2] A. Chidukwani, S. Zander and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," in IEEE Access, vol. 10, pp. 85701-85719, 2022, doi: 10.1109/ACCESS.2022.3197899

[3] Kasl, F. (2018). Cybersecurity of small and medium enterprises in the era of internet of things. The Lawyer Quarterly, 8(2).