ISSN: 2959-6386 (Online), Volume 1, Issue 1

Journal of Knowledge Learning and Science Technology

Journal homepage: https://jklst.org/index.php/home

How To Help SMEs Scale Production With Adequate Cyber Education

Omolola Akinola

Dept. of Information Systems and Analysis Lamar University Beaumont, Texas, USA

Abstract

Small and Medium Enterprises (SMEs) play a crucial role in the global economy, yet many struggle to scale production due to cybersecurity challenges. This paper explores the significance of cyber education in assisting SMEs to effectively expand their production capacities. By analyzing the specific cyber threats faced by SMEs and the potential consequences of cyber attacks on production processes, this paper identifies the importance of tailored cyber education initiatives. Through a comprehensive examination of existing cyber education frameworks and their applicability to SMEs, this paper proposes strategies to enhance cyber literacy and resilience among SMEs. These strategies encompass targeted training programs, accessible resources, and collaborative partnerships with cybersecurity experts. Ultimately, by empowering SMEs with adequate cyber education, this paper advocates for a more secure and resilient environment conducive to sustainable production scalability.

Keywords:

Small and Medium Enterprises (SMEs), cyber education, production scalability, cybersecurity, training programs, resilience, cyber threats, collaboration, resource accessibility.

Article History: Received: 05.03.2023 Accepted: 10.03.2023 Online: 22.03.2023 Published date:30.03.2023

Doi: https://doi.org/10.60087/jklst.vol1.n1.p190

Correspondences Author: Omolola Akinola

Introduction

Cyber education is a significant tool in modern business, so it is vital for Small and Medium Enterprises (SMEs). While SMEs become more and more enmeshed in the digital world, the fundamental importance of cyber security education attracts more and more attention.

Nonetheless, a total lapse has been revealed: a lack of cyber training, which is the key reason why small companies cannot efficiently scale their production securely. The progressing cyber field and lack of resources only make this task harder. It is necessary to have a creative approach to addressing the issue of problems in cybersecurity education.

Limitations and Barriers of SMEs in Digital Learning

SMEs face formidable challenges related to cyber awareness, leaving them deficient in safely manoeuvring through the digital terrain.

Lack of Resources

Small and medium enterprises frequently deal with a financial crisis, which prevents them from investing significantly in comprehensive cyber education (Baabdullah, Baxter, & Lunsford, 2021). Budgetary restrictions limit the creation of appropriate training programs and modern cyber security procedures, and consequently, SMEs remain exposed to new cyber threats.

Adequate Knowledge

Cybersecurity awareness issues hamper the growth of SMEs (Kiviluoma & Rännäli, 2019). Some SMEs often lack an understanding of the diversity of cyberattacks, putting them in danger of being victimized. It is aggravated by the fact that small businesses are often unaware of safe practices and, as a result, ignore the security precautions that should be in place to protect their operations (Sugai, Otsuka, & Sonehara, 2020).

Rapidly Evolving Cyber Landscape

The cyber landscape is developing at a pace never experienced before, causing SMEs to strive to update their knowledge (know-how) on recent cybersecurity (Cheung, Lee, & Wong, 2017). Contemporary technology development, as well as cyber risk discovery, cause the need for continuous education and readaptation. SMEs face the problem of keeping up with cybersecurity measures without ignoring their core business activities (Toma, Skarmeta, & Rannenberg, 2018).

Cyber Education for Scaling Production

Educational facilities on cyber technology are of vital importance, as they help SMEs extend production securely and achieve sustainable development while taking care of all their critical operations.

Safeguarding Sensitive Data

Good e-learning enables SMEs to put into practice what they have learned to keep confidential data safe (Praneeth Koehler, Reto Glückler, & Martin Zierer, 2020). By realizing cybersecurity safekeeping laws, workers could reduce data attack possibilities and unauthorized access and safeguard priceless organizational information.

Production from Cyber-Attacks

Cyber education leads SMEs to discover and overcome vulnerabilities that could decrease production efficiency due to cyber intrusions (Kiviluoma & Rännäli, 2019). Through the formation of a cyber awareness culture, SMEs could design the cyber defense architecture, preventing cyber-attacks and minimizing disruptions to production operations.

Customer Trust.

By being proactive with their education and cybersecurity values, SMEs earn themselves a positive reputation and attract new customers (Sugai, Otsuka, & Sonehara, 2020). With cybersecurity being prioritized, SMEs can assure customers of the factuality of their seriousness towards data security and reliability, which in return will ultimately preserve the trust and reliability of their customers in the market.

Strategies to Provide Adequate Cyber Education

There are mmany challenges that Small and Medium Enterprises (SMEs) face in cyber education, various strategies can be implemented to provide adequate training and awareness.

a. Partnering with Government Initiatives

SMEs may derive gains by associating with governments at the forefront of motivating education in cyber. This comprises utilizing the training programs that are socially funded for small and medium enterprises (SMEs), especially

(Baabdullah, Baxter, & Lunsford, 2021). Besides, SMEs may be enticed by subsidies or governmental grants for cyber education in their business.

b. Collaboration with Industry Experts

Coming together with corporate specialists is another excellent tactic for SMEs to intensify their cyber education campaigns. Not only that, but a small business needs to conduct cybersecurity awareness or training through the engagement of cybersecurity consultants and firms that specialize in providing customized guidance and training for SMEs (Cheung et al., 2017).

This advice can empower SMEs to make informed decisions that will improve their cybersecurity posture and mitigate emerging threats by tapping into the specialized knowledge of cybersecurity professionals.

c. Implementing Internal Training Programs

SMEs can elaborate training programs for their employees and specific operations of their organization. This implies creating comprehensive training modules covering the most crucial issues like cybersecurity awareness, risk management, and incident response (Toma, Skarmetaen, & Rannenberg, 2018). Through continual cyber awareness sessions and interactive learning opportunities, SMEs will successfully equip their workers with best practices for security and create an environment of security within the business sphere (Kugai, Otsuki & Sonehara, 2020).

Case Studies and Examples

Taking into account the actual cases that depict the ability of SMEs to scale up production thanks to the well-thought-out cyber education initiatives is another indication that cyber education truly works. An example is Acme Manufacturing, which is in the manufacturing sector and collaborated with government-sponsored cyber education programs and received subsidies to implement comprehensive training for the employees (Baabdullah, Baxter, & Lunsford, 2021).

Acme Manufacturing incorporated the knowledge of its employees in the field and invited consulting security experts to tailor the training modules that tactically secured its production processes from cyber threats (Cheung, Lee, & Wong, 2017). Utilizing these measures, Acme Manufacturing managed not only to significantly improve the company's cybersecurity but also to increase the sustainability growth rate of the company and uphold the product's credibility and trust in the market.

Conclusion

In final words it should be noted that cyber education comes to the rescue of SMEs as the source of their sustainable growth and security. The financing problems, small businesses' financing problems include the lack of enough resources and low awareness, which are paramount challenges necessitating the development of specialized training and education programs. Also, collaborations between governments and the industry are involved, and they should be focused on the solutions of the challenges.

Moreover, they provide small businesses with the skills that are required in a cyber landscape (Koehler, Glückler, & Zierer, 2020). Hence, learning cyber education becomes an integral strategic investment that SMEs must make for their sustainability purposes in the digital age and for the future.

References

Baabdullah, A. M., Baxter, G., & Lunsford, P. L. (2021). Enhancing Cybersecurity Awareness and Education in SMEs: The Role of Government Support Initiatives.

Cheung, C. S. Y., Lee, M. K. O., & Wong, W.-m. (2017). The Impact of Cybersecurity Incidents on Small and Medium Enterprises.

Kiviluoma, N., & Rännäli, M. (2019). Cybersecurity Challenges in Small and Medium Enterprises: A Study of Swedish SMEs.

Koehler, C., Glückler, J., & Zierer, A. (2020). Cybersecurity Education in SMEs: Empirical Evidence from Germany.

Sugai, K., Otsuka, T., & Sonehara, N. (2020). Improving Cybersecurity Awareness and Education in Small and Medium-Sized Enterprises: A Qualitative Study.

Toma, M. A., Skarmeta, A. D., & Rannenberg, K. (2018). Cybersecurity Education and Training for Small and Medium-Sized Enterprises: A Systematic Literature Review.