ISSN: 2633-4828 Vol. 5 No.4, December, 2023

International Journal of Applied Engineering & Technology

AN EXAMINATION OF CYBER SECURITY GOVERNANCE AND POLICY FOR SMALL AND MEDIUM ENTERPRISES IN THE CONTEXT OF INDUSTRY 5.0

Rajesh Verma
Assistant Professor, International Institute of Professional Studies (IIPS), Devi Ahilya Vishwavidyalaya, Indore, Madhya Pradesh, India
rv097227@gmail.com

ABSTARCT

Small and medium-sized enterprises (SMBs) make up a sizable portion of the economies of many countries; but, as of this writing, SMBs are not implementing cyber security to a sufficient degree, leaving them open to cyberattacks. Furthermore, the exploration considers the methodologies embraced by Tamil Nadu and Maharashtra and assesses the job that government strategies and mandates have in advancing cyber security rehearses among SMEs. Using a mixed techniques examination that incorporates interviews with specialists and SME proprietors, the examination features difficulties and presents open doors for improving cyber security policy and governance in the two nations. The discoveries feature the requirement for fitting arrangements because of the assorted social and monetary conditions in Tamil Nadu and Maharashtra. The appraisal centers around SMEs in Maharashtra and their consistence with the Essential Cyber Security Controls (ECC) guidelines, explicitly analyzing the mindfulness and execution of cyber security measures. Furthermore, it analyzes the care and consistency of cyber security estimates that are presently set up in Tamil Nadu and investigates genuine heading chronicles pointed toward assisting SMEs with accomplishing better cyber security rehearses. This paper gives a near examination an emphasis on governance and policy between Tamil Nadu and Maharashtra. It additionally acquaints a few proposals with fortify cyber security mindfulness and schooling, keep up with regulatory structures, and backing public-private organizations in the battle against cyber security dangers in the industry. 5.0-Landscape.

Keywords:*Cyber Security, Governance, Policy, Small, Medium, Enterprises, Industry 5.0, Essential Cyber Security Controls, Small-to-medium sized businesses,Small and medium enterprises (SMEs)*

1. INTRODUCTION

Small and medium-sized businesses (SMEs) have interesting cybersecurity challenges. They typically miss the mark on assets and skill important to appropriately get to their systems and data, delivering them exposed against cyberattacks. SMEs make up a significant piece of the economy in Grains, and the region's general development and thriving rely upon their prosperity. The Welsh Government (WG) has done whatever it takes to help SMEs around here since they perceive the significance of cybersecurity. For instance, the government has arranged programs and given endowments to assist SMEs with propelling their cybersecurity pose. Furthermore, the government has sent off missions to urge SMEs to embrace best practices, such the Cyber Action Plan, and to turn out to be more aware of cybersecurity. Be that as it may, regardless of these endeavours, numerous SMEs in Grains are really experiencing issues executing powerful cybersecurity securities. The absence of care and attention to the significance of cybersecurity among SMEs is one significant test.

Numerous SMEs could not completely value the dangers presented by cyberthreats, or they could miss the mark on assets important to manage these dangers. An extra boundary is the expense of carrying out cybersecurity shields. Numerous SMEs might find it challenging to manage the cost of the hardware and administrations important to safeguard their systems and data, particularly assuming they are as of now working on limited spending plans. Along these lines, SMEs might find it challenging to persuade accomplices and themselves that the cost of cybersecurity safeguards is legitimate. At long last, to help them execute and deal with their security measures, SMEs might experience difficulty finding and holding talented cybersecurity trained professionals. Because of the profoundly particular nature of cybersecurity, SMEs might miss the mark on assets to rival bigger

associations for these significant recruits. The focal point of this study is on SMEs' impression of cybersecurity and the difficulties and hindrances that exist today.

As of late, high level change inflows have made it harder for small and medium-sized businesses (SMEs) to embrace and integrate constantly developing innovations into their activity plans. Mechanical progressions have opened up fascinating monetary open doors, whether it be in web-based shopping or overseeing supply chains of organizations. Notwithstanding, they have likewise delivered new difficulties that have changed progressive plans, the capacity to oversee data, and extra wellspring of hazard. Without a doubt, arising difficulties, for example, cyber-betting and data security have brought about boundless monetary and nonfinancial misfortunes. Thus, it is believed that SMEs face comparable levels of cybersecurity risks to their larger counterparts; but, due to their limited resources and capabilities, they are more vulnerable to cyberattacks. In other words, preparing and understanding cyber risk become essential for small business success and survival.

Given that researchers have recently grown more aware of cybersecurity, certain shortcomings in surviving exploration have been identified. Primarily, a vast array of cybersecurity literature has examined the risk associated with board systems, specific problems, hierarchical structures, mindfulness, and relief options in large corporations. Nevertheless, there is a dearth of substantial knowledge regarding the extent to which SMEs handle cyber risks. SMEs are thought to be a prime target for cyber aggressors looking to expand into larger partners, as they are frequently important partners of larger companies. Thusly, extra exploration is expected to investigate the degree of readiness, risk appraisal methods, and defensive capacities in handling cybersecurity issues inside small businesses, for example, e-following SMEs (online retailing SMEs that offer thing/administration proposing to customers through the Internet). Given the expected effect of cyber gambles, electronic retailing SMEs are among the biggest adopters of web and correspondence developments. Subsequently, it is basic to distinguish the dangers these SMEs face and direct a setting centered study of them.

2. LITERATURE REVIEW

Krahl (2019)explores the intricate field of cybersecurity as it relates to small and medium-sized enterprises (SMBs). Small and medium-sized businesses often have significant challenges when it comes to safeguarding their digital assets due to asset requirements and a lack of dedicated cybersecurity expertise. Krahl's hypothesis looks at the specific risks that SMBs face and examines various practices and technological advancements that can be used to lessen those risks. This investigation significantly advances knowledge of and attention to the vulnerabilities existing in the cybersecurity space by providing SMBs' perspective of the landscape.

Mackey and Gass (2023)offer a fascinating exploration of mental cycles within the framework of second-request cybernetics, focusing on the situations that BANI (Fragile, Spry, Nonlinear, and Deficiently Determined) attributes. This investigation provides a novel perspective on comprehending and managing complex systems, particularly in the context of rapidly evolving mechanical environments. Through examining the relationship between mental cycles and cybernetic norms, Mackey and Gass provide valuable insights into how associations can adapt and thrive in challenging environments that are fraught with risk and unpredictability.

Nieto, Acien, and Fernandez (2019)offer a fascinating exploration of mental cycles within the framework of second-request cybernetics, focusing on the situations that BANI (Fragile, Spry, Nonlinear, and Deficiently Determined) attributes. This investigation provides a novel perspective on comprehending and managing complex systems, particularly in the context of rapidly evolving mechanical environments. Through examining the relationship between mental cycles and cybernetic norms, Mackey and Gass provide valuable insights into how associations can adapt and thrive in challenging environments that are fraught with risk and unpredictability.

Panteli et al. (2023)explore the nuances of organising limit traversing tasks for internal association cybersecurity. The "grouping felines" depiction effectively captures the challenges inherent in adjusting to various partners and advances a common cybersecurity goal. This investigation sheds light on the challenges of coordinating work and communication across hierarchical boundaries, highlighting the need of developing a strong cybersecurity culture in order to effectively manage cyber risks. Panteli et al. provide valuable insights into cybersecurity's limit-

crossing features, which are useful for professionals and policymakers seeking to enhance hierarchical flexibility in the face of growing cyber threats.

Boese (2020)investigates the particular difficulties that small businesses experience in accomplishing consistence with the Payment Card Industry Data Security Standard (PCI DSS). Consistence with PCI DSS is essential for associations that handle payment card data, yet small businesses often battle to explore the complicated prerequisites because of restricted assets and aptitude. Boese's postulation gives a complete investigation of the obstructions to PCI DSS consistence looked by small businesses and offers pragmatic proposals for defeating these difficulties. By tending to the interesting necessities and limitations of small enterprises, this examination adds to further developing cybersecurity rehearses and regulatory consistence inside this sector.

Keller et al. (2005) Investigate small business data security risks and procedures, realising the value of comprehending the cybersecurity environment from their perspective. Although this was a relatively early analysis, its findings are still important today, highlighting the prevalence of security flaws and the need for specialised risk mitigation strategies in small business environments. Keller et al. establish the groundwork for developing more potent cybersecurity frameworks tailored to the unique needs and constraints of small firms by identifying common threats and examining current security practices.

3. METHODOLOGY

In order to compile and analyse the necessary data, the investigation used a mixed methods approach that combined mandatory and optional data assortment strategies. The degree, points, and objectives of the test determined which methods were used. A study poll was designed with the express purpose of gathering vital data about the Maharashtra SME landscape. The survey underwent a comprehensive friend survey cycle to ensure that it was relevant and responsive to small and medium-sized enterprises in Maharashtra. The questions were modified to better reflect the objectives of the exploration. The Qualtrics platform was used to manage the review, facilitating data collection and analysis. The questions were presented to the respondents in an eye-to-eye interview format to ensure clarity and facilitate their understanding and response. By using effective data collection and analysis techniques, using Qualtrics as a platform provided significant capabilities in bridging information gaps.

Notwithstanding the vital data, the examination consolidated supporting data from a careful composing review. Various scattered sources, including books, government distributions, papers, periodicals, and journals, were carefully analyzed to assemble dependable data pertinent to the field of request. Securing discretionary data that straightforwardly related with the test targets showed specific difficulties. In the long run, the mix of the audit's basic data and the goodies of information from the assistant assets gave the examination greater believability and credibility.

The assessment planned to create new data and bits of knowledge that supplement the current composition by utilizing a mix of mandatory and discretionary data assortment techniques. Concentrating on SME proprietors and senior authoritative staff with SME data in Maharashtra was one of the significant data sets. Notwithstanding, the examination of historical conveyances and the coordination of data from the respondents in Tamil Nadu were important for the examination of assistant data. This complete technique took into account a powerful report, empowering the examination to genuinely accomplish its goals.

By empowering a decent exploration and guaranteeing an extensive investigation of the investigation issue, the use of these assessment methods of reasoning upgraded the legitimacy and believability of the investigation disclosures. The mix of mandatory and deliberate data assortment techniques gave important experiences into the cyber security policy and governance climate for SMEs concerning Industry 5.0, adding to the collection of information around here.

3.1. Research Hypotheses

The resulting assessment hypotheses were intended to examine the similitudes and contrasts between SMEs in Maharashtra and Tamil Nadu as to cyber security governance and policy execution, as well as the effect of Industry 5.0 on these boundaries:

H1: Maharashtra SMEs will have greater cyber security resilience if they have robust cyber security governance and policy implementation.

H2: Higher cyber security resilience will also be demonstrated by Tamil Nadu SMEs with strong cyber security governance and policy execution.

H3: Maharashtra's implementation of Industry 5.0 SMEs' emphasis on customized supply chains and human-centered production may cause them to change how cyber security governance and policies are implemented.

H4: In a similar vein, Tamil Nadu SMEs' adoption of Industry 5.0 may have an impact on the governance and implementation techniques of cyber security policies.

H5: There are anticipated variations in the governance and execution of cyber security policies between SMEs in Tamil Nadu and Maharashtra, which are probably impacted by regionally specific cultural, legal, and contextual elements.

4. RESULTS

4.1. Maharashtra Results

4.1.1. Section One

The results and analysis of the investigation are sorted and dissected in this part. The assortment of data in regards to the respondent's experience and company were remembered for the principal section. The review included segment-style questions about the SME respondent's industry, work, maturity, orientation, and educational background in addition to mature questions.

This Figure 1 provides insight into the composition of a particular group or test population by breaking down the answers according to several professional and segmental variables. We ought to thoroughly understand each variable:

- **Education Level**: The respondents' conveyance based on their capacity to instruct is displayed in the table. 32% of respondents had graduate degrees, whereas 50% of respondents had four years of college education. Four percent have completed secondary education, while seven percent either have PhDs or are classified as "Other," which could include professional qualifications, partner degrees, or confirmations.
- **Age**: The age distribution of the responses indicates a somewhat young population, with the majority (60%) falling between the 26–35 age range. This is lagging behind by 11% in the 45–55 age group and 16% in the 36–45 age group. The percentages decrease for more experienced age groups; only 4% of adults 56 to 65 and 9% of adults 18 to 25 fall into these categories.
- **Gender**: Male respondents make up the majority of the data on orientation conveyance (75% of the sample). However, 25% of all respondents are female, making up the total population under study.
- **SME Industry**: This section provides tidbits of information about the companies that employ the respondents, specifically focusing on Small and Medium-sized Enterprises (SMEs). The majority of respondents (48%) are employed in the administrative sector, indicating a diverse range of administratively oriented firms. Following with 8% of responders each, the training and retail sectors are followed by tourism with 10%. Smaller portions of the responder pool comprise various industries such as food, wellness, promoting, showcasing, oil & gas, and development, with percentages ranging from 3% to 5%.

Figure 1 depicts a predominantly male population that is reasonably youthful and has completed four years of college. They are primarily used in assistance-related SMEs, but there are also representations from other industries. Comprehending these socioeconomic concepts can facilitate appropriate methods and methodologies while incorporating or emphasising this particular group of people for various objectives, such as advocacy, policy formation, or educational initiatives.

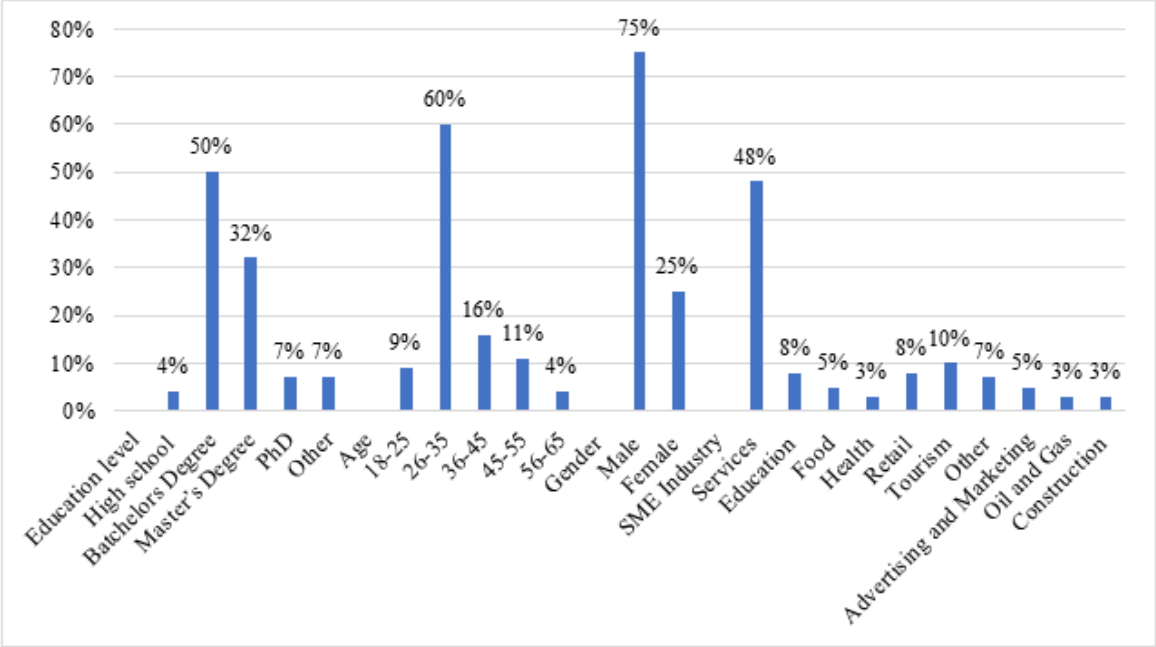

Figure 1: Graphs Showing Industry Distribution and Demographics

The occupations of the SME respondents are depicted in Figure 2, with 30% of respondents being entrepreneurs, 18% being chiefs, and 10–13% being administrators, deals, and managers.

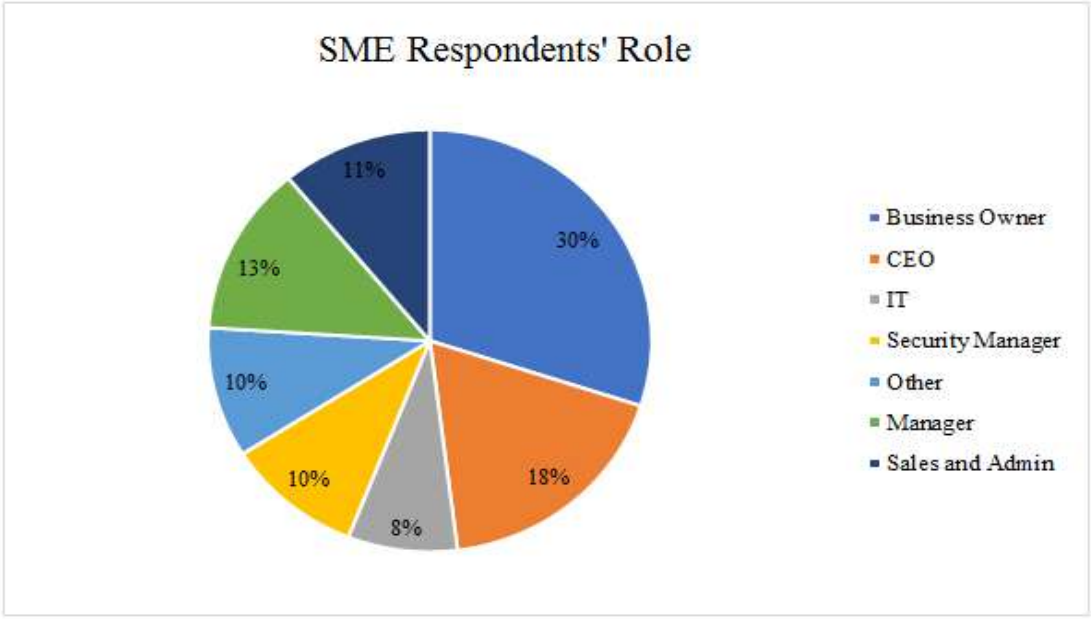

Figure 2: SME Respondents' Role.

The first segment clearly demonstrated the wide range of SME respondents' occupations, ages, orientations, industries, and levels of training. The unique evidence of these elements is critical to comprehending the socioeconomics and the image of the SMEs under review in this analysis. In closing, 91% of the SME respondents came from foundations of information and schooling and had advanced education. Given this, the supplementary data collected in the ensuing sections may influence the way in which the respondents answered and replied.

4.1.2. Section Two

In the concentrate's subsequent segment, members were posed a progression of inquiries on Monsha'at, Maharashtra's SME Authority, the state's National Cyber Security Agency (NCA), and the ECC report and its consistency. Table 1 presents SMEs' reactions to these inquiries.

Table 1: A scope of requests to see whether SMEs accept they are focuses for cyberattacks, as well as their insight into Monsha'at, NCA, and ECC consistence.

Question	SMEs an Attacker's Target	SME Awareness of Monsha'at	SME Awareness of NCA	Are You Aware of ECC?	If Yes, Do You Comply?
Yes	38%	67%	94%	60%	54%
No	62%	33%	6%	40%	46%

Measuring and comprehending Monsha'at consciousness was crucial, as was observing the effects of the organisation in providing SME enterprises with the support they require to maintain their security. Figure 3 shows more precise translations of the administrations used or not used by the SME respondents in this overview.

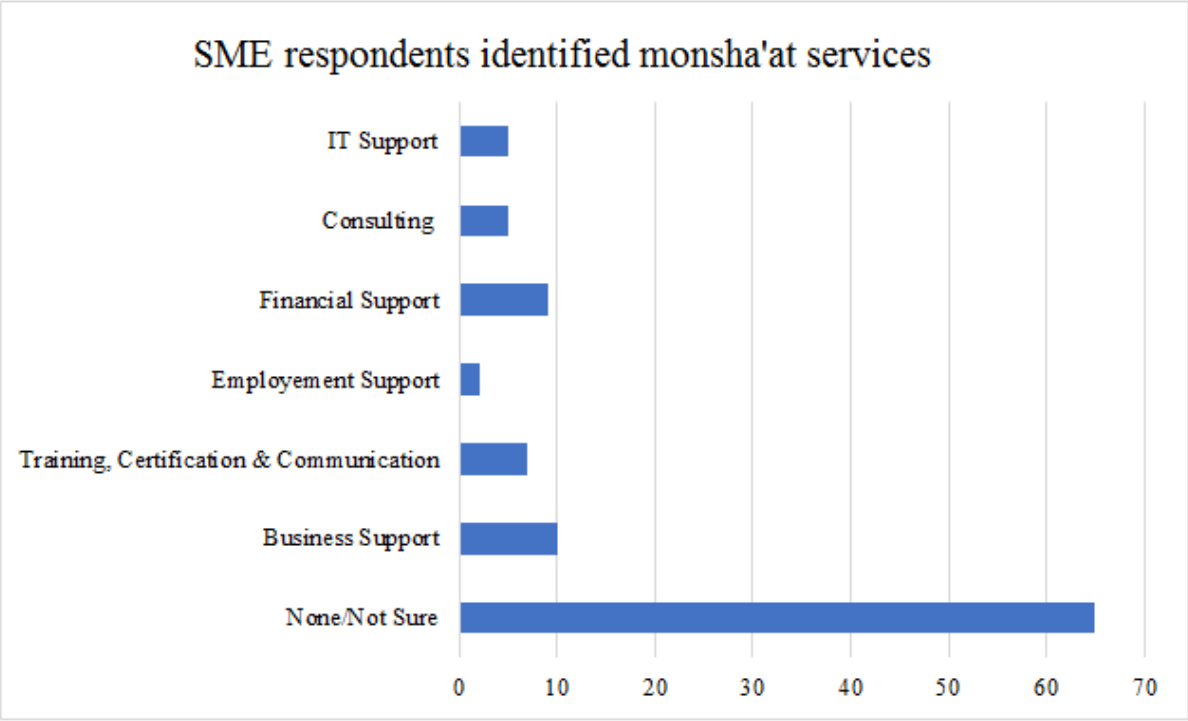

Figure 3: Services offered by Monsha'at recognised by SME responders.

Of the participants who indicated they gave their authorization to use the Monsha'at administration, sixty-five percent claimed they had no idea what the assistance was or had never used it. Nine to ten percent of the participants availed themselves of the available Monetary and Business support, while seven percent relied on

Monsha'at for interview preparation, exchanges, and occasionally business accreditations. Merely 5% of the participants used Monsha'at's counselling packages and IT support. Although Monsha'at provides a plethora of services and initiatives for businesses to leverage, the majority of participants only utilised a portion of the association's data. The levels described at the time of learning that you were being pursued were comparable throughout this level. According to Figure 4, which depicts them being pursued online, the results here indicate that 20% of SME respondents said they were not afraid, slightly terrified, scared, or extremely afraid.

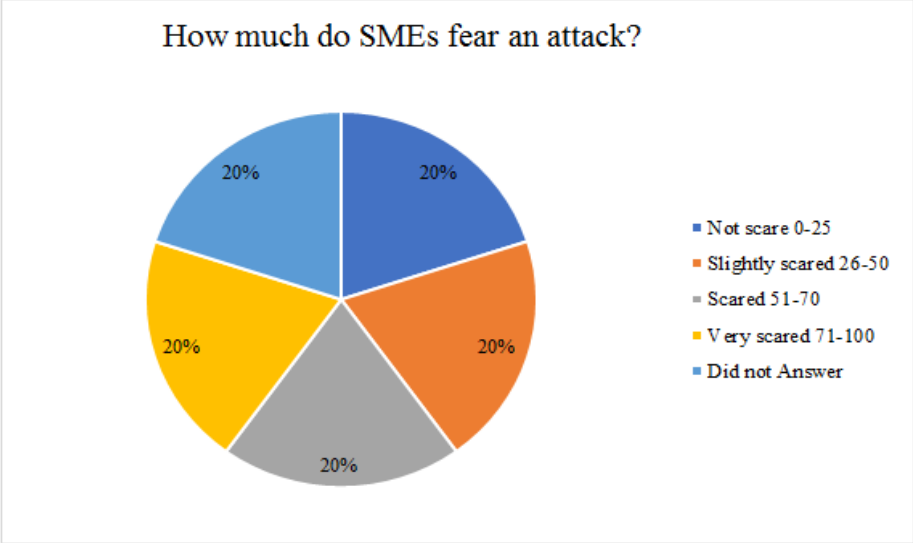

Figure 4: How much do SMEs fear an attack?

Figure 5 exhibits that most of SMEs utilized On Reason (41%) or the Cloud choice (42%) as their server region. A couple of SMEs chose Combination and Off Reason, at 5% and 8%, separately. The discoveries were blended in that while cloud security was improving, numerous SME respondents were truly utilizing an On Premises arrangement that conveyed a critical gamble. Future exploration might investigate the likelihood that the quantity of SMEs utilizing distributed computing will increment or reduction. This is on the grounds that there are a ton of choices to be made about what security controls are essential and how best to design rules and mindfulness crusades around these controls for SMEs.

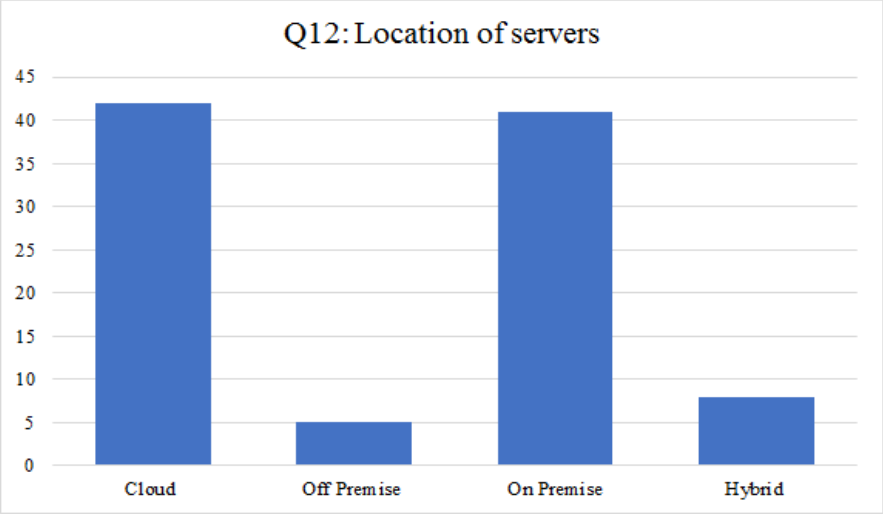

Figure 5: Question 12: Where Are the Servers?.

Table 6 obtained information on their thoughts on the National Cyber Security Agency (NCA) of Maharashtra. This result had particular significance as it demonstrated the extent to which the government push was noteworthy and acknowledged throughout Maharashtra. Soon after the colleague with the NCA, the subject of the ECC record and the SMEs' adherence to the report as a benchmark came up. A shift in mindfulness was brought about by the 60/40 sharing of this result. It's possible that it will be contacted because, given that it's a government initiative, all SMEs in Maharashtra should be aware of this data. The clarifications for the people who expressed they wouldn't concur were missed, however they give a captivating topic to additional examination. In this section of the controls, twelve questions were asked to demonstrate that SMEs were endorsing the ECC report as part of the ECC consistency. The results are displayed in Figure 6 and Table 2.

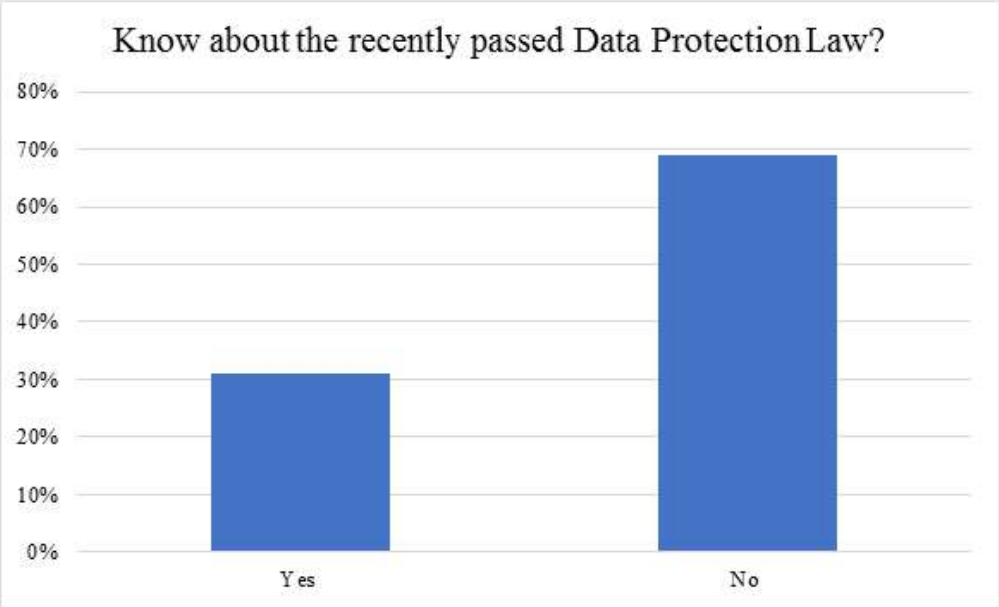

Figure 6: Recognising the new legislation protecting personal data.

Table 2: Compliance with ECC (Questions 1–11).

Question	Anti-Virus (1)	Regular Updates (2)	Governance and Policy (3)	Risk Assessment (4)	Cyber Security Strategy (5)	Cyber Security Department (6)	Cyber Security Consideration (7)	Vulnerability Scanning (8)	Auditing (9)	Security Awareness Program (10)	Regular Backup (11)
Yes	88%	85%	63%	53%	49%	26%	56%	56%	52%	43%	82%
No	12%	15%	37%	47%	51%	74%	44%	44%	48%	57%	18%

The ECC record made it abundantly evident in its elements that SMEs and businesses should exercise caution and security whenever they utilise the internet in order to prevent cyberattacks. Notwithstanding, it was likewise obvious that while half of the SMEs were observing the guidelines, the other half missed the mark on clear strategy. In a perfect world, the situation would have been exceptional on the off chance that these SMEs had exhibited a more noteworthy level of consistency with the ECC record, recommending that extra conversations around this consistency might just expand the ECC's care and use.

5. CONCLUSION

The assessment of the cyber security governance and policy structures in Tamil Nadu and Maharashtra gives significant experiences into upgrading cyber security for small and medium-sized enterprises (SMEs). The analysis features the significance of government backing and care lobbies for SMEs through unprecedented

obligations, featuring Maharashtra's advancement with the Essential Cybersecurity Controls (ECC) report and recognizing execution holes and care among SMEs. Our cognizance of the difficulties looked by SMEs in Maharashtra is expanded by extra clarification of cultural issues, security points of view, and explicit weaknesses in the Middle East. Within the context of Industry 5.0, where technological advancements amplify cyber threats, the investigation highlights the necessity of robust governance and regulatory frameworks to safeguard small and medium-sized enterprises and foster growth. The review makes a significant contribution to the rational information in cyber security governance and policy through its practical approach and noteworthy suggestions. It anticipates advancing cyber security in the evolving context of Industry 5.0, supporting the development of the computerised economy, and strengthening SME flexibility.

REFERENCES

1. Alsahafi, T.; Halboob, W.; Almuhtadi, J. Compliance with Saudi NCA-ECC based on ISO/IEC 27001. Teh. Vjesn. 2022, 29, 2090–2097.
2. Bada, M.; Nurse, J.R.C. Developing cyber security education and awareness programmes for small- and medium-sized enterprises (SMEs). Inf. Comput. Secur. 2019, 27, 393–410.
3. C. Bucolo. Get PCI Compliance Right the First Time. PCI Compliance Guide. Accessed: Aug. 2, 2020. [Online]. Available: https://www. pcicomplianceguide.org/get-pci-compliance-right/
4. Dawson, M. 2019 An Argument for Cyber security in Maharashtra. Land Forces Acad. Rev. 2022, 27, 78–83.
5. Eilts, D., & Levy, Y. (2018). Towards an empirical assessment of cybersecurity readiness and resilience in small businesses. KSU Proceedings on Cybersecurity Education, Research and Practice. https://digitalcommons.kennesaw.edu/ccerp/2018/practice/2
6. Forte, P.; Schiraldi, M.M.; Petrescu, R.V. Industry 4.0 Revolution and Its Impact on Industrial Robotics. In Robotics in Industry; Springer: Cham, Switzerland, 2023; pp. 3–17.
7. Grange, C.; Beerepoot, M.; van Klink, B. The brittleness of socio-technical systems: Towards a conceptualization. Technol. Forecast. Soc. Chang. 2023, 176, 121108.
8. Heidt, M.; Gerlach, J.P.; Buxmann, P. Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. Inf. Syst. Front. 2019, 21, 1285–1305.
9. Ishizaka, A., & Resce, G. (2020). Best-worst PROMETHEE method for evaluating school performance in the OECD's PISA project. Socio-Economic Planning Sciences, **73**, 100799. https://doi.org/10.1016/j.seps.2020.100799
10. J. F. Carias, M. R. S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, ‘‘Systematic approach to cyber resilience operationalization in SMEs,’’ (in English) IEEE Access, vol. 8, pp. 174200–174221, 2020, doi: 10.1109/ACCESS.2020.3026063.
11. K. E. Krahl, ‘‘Cybersecurity and small to medium business,’’ M.S. thesis, Utica College, ProQuest Dissertations Publishing, 2019.
12. Mackey, A.; Gass, S.M. Second-order cybernetics of cognitive processes: An analysis of BANI environments. J. Manag. Inf. Syst. 2023, 40, 194–220.
13. Nieto, A., Acien, A., & Fernandez, G. (2019). Crowdsourcing analysis in 5G IoT: Cybersecurity threats and mitigation. Mobile Networks and Applications, **24**(3), 881–889. https://doi.org/10.1007/s11036-018-1146-4
14. Panteli, N.; Procter, R.; Mowbray, M.; Poschen, M. “It’s like herding cats”: Coordinating boundary-spanning work for cybersecurity in organizations. J. Assoc. Inf. Syst. 2023, 24, 467–497.

15. R. F. I. V. Boese, ‘‘PCI DSS compliance challenges for small businesses,’’ M.S. thesis, Utica College, ProQuest Dissertations Publishing, 2020, Art. no. 27672228.

16. S. Keller, A. Powell, B. Horstmann, C. Predmore, and M. Crawford, ‘‘Information security threats and practices in small businesses,’’ (in English) Inf. Syst. Manag., vol. 22, no. 2, pp. 7–19, Mar. 2005, doi: 10.1201/1078/45099.22.2.20050301/87273.2.

17. T. Tam, A. Rao, and J. Hall, ‘‘The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses,’’ (in English) Comput. Secur., vol. 109, Oct. 2021, Art. no. 102385, doi: 10.1016/j.cose.2021.102385.

18. Verizon. (2016). Data Breach Investigations Report. [Online]. Available: https://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/ 10/2016/10/2b_Verizon_Data-Breach-InvestigationsReport_2016_Report_en_xg.pdf

19. Widup, S.; Hylender, D.; Bassett, G.; Langlois, P.; Pinto, A. Verizon: Data breach investigations report 2020. Comput. Fraud Secur. 2020, 2020, 4.

20. Zec, M. Cyber Security Measures in SMEs: A research of IT Professionals Organisational Cyber Security Awareness. Master’s Thesis, Linnaeus University, Växjö, Sweden, 2015.