HOW DO SMES PERCEIVE CYBERSECURITY MEASURES TO PROTECT CUSTOMER DATA?

Musaed Al-Fareh , Pierezza Edoardo, Davila Cadena Felipe, Roelevink Bread

INTRODUCTION

Limited resources make it challenging for SMEs to defend against cyber threats. This poster explores these challenges and offers strategies for enhanced SME cybersecurity.

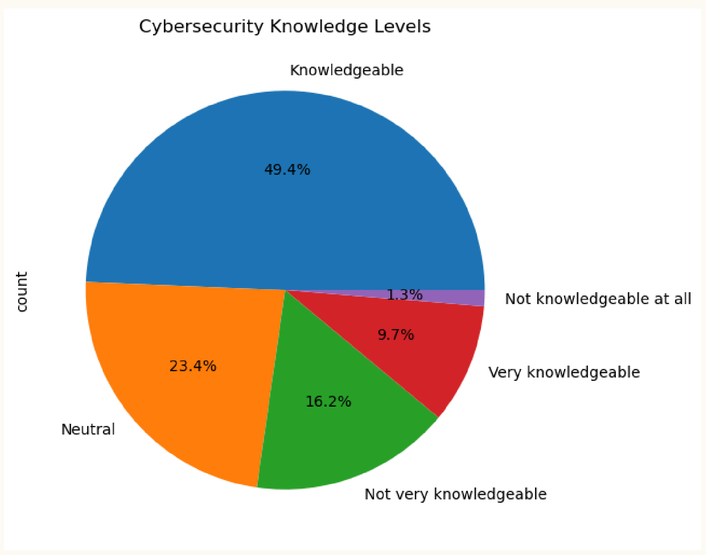
OBJECTIVE

- identify key barriers to cybersecurity adoption in SMEs
- Analyze current data protection practices in SMEs
- Provide actionable recommendations for enhancing SME - cybersecurity within sector-specific resource constraints

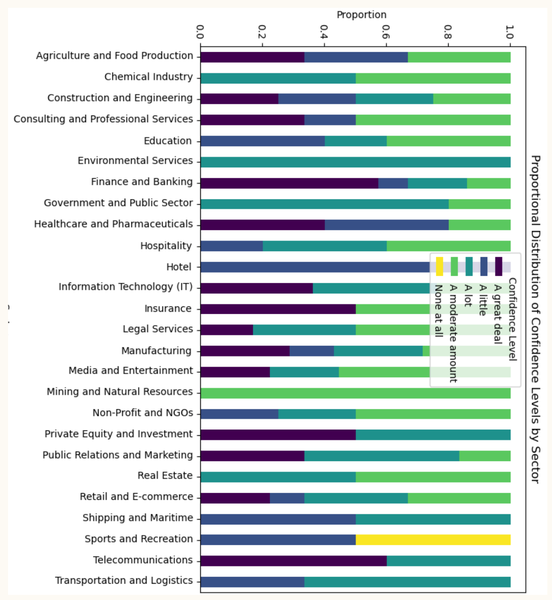
METHODOLOGY

- Data Collection: Semi-structured interviews and surveys from SME leaders across sectors.
- Analysis:
- Quantitative: EDA, descriptive statistics, and Chi-Square tests on survey data to identify patterns by company size, sector, and awareness.
- Qualitative: Thematic analysis of interview data to reveal sector-specific cybersecurity practices.

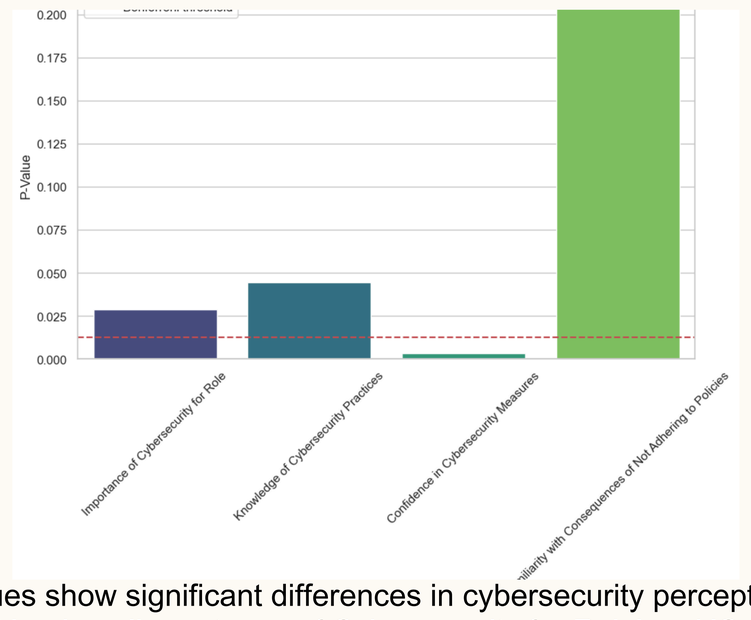
KEY FINDINGS AND ANALYSIS



Survey shows 49.4% of SME leaders feel 'Knowledgeable,' while others display a range of awareness levels, indicating potential areas for targeted training.



The chart shows the distribution of confidence in cybersecurity measures across various sectors. Industries like Finance, IT, and Government display high confidence, with most employees reporting "A great deal" or "A lot" of confidence. In contrast, sectors such as Agriculture, Public Relations, and Sports show lower confidence levels, with more responses in the "A little" or "None at all" categories. This suggests that highly regulated sectors feel more secure, while others may lack the resources or infrastructure for strong cybersecurity.



T-test p-values show significant differences in cybersecurity perceptions among SME leaders. 'Importance of Cybersecurity for Role' and 'Confidence in Cybersecurity Measures' meet the Bonferroni threshold, while 'Familiarity with Policy Consequences' does not, highlighting a potential gap in awareness.

RECOMMENDATION

- Enhance Training Programs: Implement sector-specific cybersecurity training to improve knowledge and confidence in cybersecurity measures.
- Raise Awareness of Policy Consequences: Address gaps in understanding the impact of not adhering to cybersecurity policies through targeted awareness campaigns.
- Develop Tailored Cybersecurity Solutions: Create adaptable cybersecurity strategies to meet the unique needs of high-risk sectors like IT, Manufacturing, and Finance.

CONCLUSION

Key Takeaways: SMEs show varying cybersecurity knowledge and confidence levels, with specific policy awareness gaps.

Outcome: Research indicates a need for customized, industry-specific cybersecurity approaches.

Future Implications: Improved training and awareness initiatives can enhance SMEs' resilience to cyber threats, fostering a more secure digital landscape for smaller businesses.