Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 4 | April 2025 -Peer-Reviewed Journal

CYBERSECURITY THREATS AND RISK MANAGEMENT IN SMALL AND MEDIUM-SIZED ENTERPRISES

Jacob M[1], Jithin Johnson[2], Gokul K[3], Dr. Chandra Shekhar[4]
[1]*22DBCOM061, VI SEM B.COM, School of Economics and Commerce, CMR University*
[2]*22DBCOM065, VI SEM B.COM, School of Economics and Commerce, CMR University*
[3]*22DBCOM053, VI SEM B.COM, School of Economics and Commerce, CMR University*
[4]*Assistant Professor, School of economics and commerce, CMR University*

ABSTRACT
This research looks into the escalating cybersecurity threats confronting Small and Medium-sized Enterprises, specifically considering their often limited cybersecurity infrastructure and resource constraints. The investigation scrutinizes prevalent and emerging threats such as phishing attacks, ransomware, data breaches, and insider risks. By identifying the unique vulnerabilities inherent in SMEs, the study analyzes the potential repercussions of cyber incidents on their operational continuity, financial stability, and public image. Furthermore, this research explores effective risk management strategies tailored for SMEs, including employee cybersecurity training, the adoption of relevant cybersecurity frameworks, the implementation of budget-conscious security technologies, and strategic partnerships with external cybersecurity experts. The ultimate aim is to empower SMEs to cultivate robust digital defenses as they expand their operations and foster a heightened understanding of the evolving threat landscape.

INTRODUCTION

Currently, Small and Medium-sized Enterprises rely heavily on technology for their operations, customer interactions, and the storage of sensitive data. While digital transformation enhances productivity and connectivity, it also makes them vulnerable to various security threats. Unlike larger corporations, SMEs often lack the financial and technical resources to establish robust security measures, placing them at significant risk. They commonly encounter cyber threats such as phishing attacks, ransomware, data breaches, denial of service attacks, and others, which can lead to substantial financial losses, operational disruptions, and damage to their reputation.

Despite this growing risk environment, many SMEs show low levels of awareness regarding cybersecurity practices and have limited preparedness against these threats. Many seem to believe they are too small to be targeted by cyberattacks, leading to complacency. However, statistics indicate that cybercriminals frequently target SME-level businesses, exploiting existing security weaknesses and human errors.

This paper will examine the nature of cybersecurity threats and the importance of risk management strategies for SMEs. By identifying vulnerabilities and potential impacts, and by implementing adaptable and affordable solutions, SMEs can strengthen their cyber resilience and ensure business continuity within a challenging threat landscape.

RESEARCH GAP

The lack of research specifically focused on cybersecurity for small and medium-sized businesses is a problem because these companies often don't have the money or technical skills to put strong security in place. Many owners and employees also don't realize how much at risk they are or understand basic cybersecurity practices. SMEs face unique threats, especially because they're often connected to bigger companies and are using more cloud services and internet-connected devices without knowing how to properly secure them. The cybersecurity tools and advice that exist are often designed for big companies and don't fit the needs or budgets of smaller ones. Because cyberattacks are constantly getting more advanced, there's a continuous need for research to find simple, affordable ways to protect SMEs. Basically, we need to better understand the specific cybersecurity issues SMEs face and come up with practical, budget-friendly solutions they can actually use.

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 4 | April 2025 -Peer-Reviewed Journal

OBJECTIVE

1. This study will investigate the most prevalent types of cybersecurity threats targeting small and medium enterprises.
2. The research will analyze the technological, organizational, and human elements that contribute to the vulnerability of SMEs to cyberattacks.
3. This paper aims to assess the current level of cybersecurity awareness and preparedness among owners and employees within small and medium enterprises.
4. The study will evaluate the effectiveness of existing cybersecurity measures and risk management practices currently implemented in SMEs.
5. This research seeks to identify the specific challenges that SMEs encounter when establishing comprehensive and adequate cybersecurity measures.
6. The paper will recommend cost-effective and practical risk management strategies specifically tailored to the needs and capabilities of small and medium-sized businesses.

METHODOLOGY

The methodology for studying cybersecurity threats and risk management in Small and Medium-sized Enterprises will involve a mixed-methods approach. Initially, a comprehensive literature review will be conducted to identify prevalent cyber threats targeting SMEs, analyze their unique vulnerabilities, and examine existing risk management frameworks and best practices relevant to this sector.

Subsequently, empirical data will be collected. This will likely involve surveys distributed to a diverse sample of SME owners and employees to assess their cybersecurity awareness, preparedness levels, and the current state of their implemented security measures. Qualitative data will be gathered through semi-structured interviews with IT professionals, business owners, and potentially cybersecurity experts working with SMEs to gain deeper insights into the specific challenges they face in establishing and maintaining effective cybersecurity.

The collected quantitative data from surveys will be analyzed using statistical methods to identify trends and correlations regarding threat exposure, vulnerability factors, and the effectiveness of current security practices. Finally, the findings from both quantitative and qualitative data will be triangulated to provide a comprehensive understanding of the cybersecurity landscape for SMEs. This integrated analysis will inform the development of cost-effective and pragmatic risk management strategies tailored to the specific needs and capacities of SMEs, ultimately aiming to enhance their cyber resilience.

RESULTS

Overall, the surveyed SMEs generally demonstrated a moderate level of awareness regarding cybersecurity threats. However, a concerning number of these businesses reported experiencing a cybersecurity incident within the past three years. The impact of these incidents commonly included financial losses, data breaches, and disruptions to their business operations.

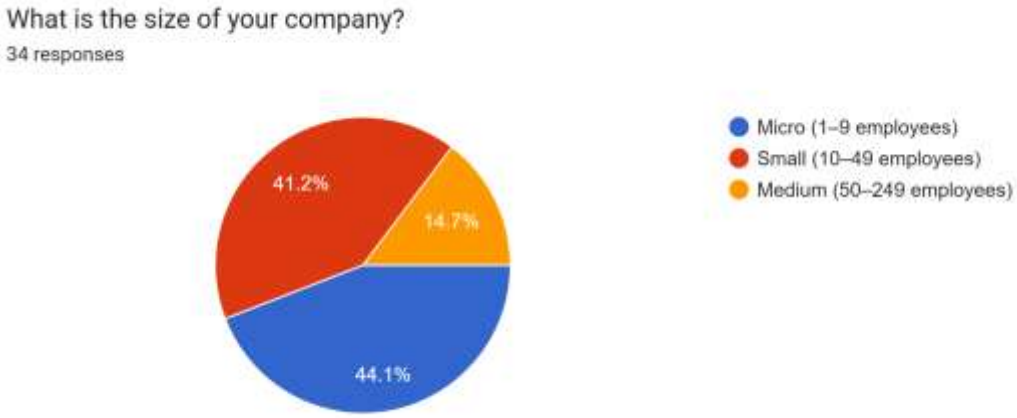
While a notable portion of the surveyed companies had established cybersecurity policies, a significant number did not. Similarly, regular cybersecurity risk assessments were not consistently conducted across all respondents, with some performing them only occasionally or not at all.

The most prevalent cybersecurity measures in use were basic tools like antivirus software and firewalls. Adoption rates for more advanced security measures, such as data encryption and multi-factor authentication, were lower. Our interpretation of the collected data highlights the key challenges SMEs face in managing cybersecurity risks. These prominently include limited financial resources allocated to cybersecurity, a lack of dedicated or skilled IT staff, and insufficient cybersecurity awareness among employees. The rapidly evolving nature of cyber threats was also identified as a significant ongoing challenge for these businesses.

In summary, our data collection and interpretation indicate that while SMEs have some level of awareness, they frequently experience cyber incidents with tangible negative impacts. Their cybersecurity posture is often basic, and they face significant hurdles – primarily financial, staffing, and awareness-related – in implementing more robust protections against an ever-changing threat landscape.

"Visual Representation of Data interpretation from the survey"

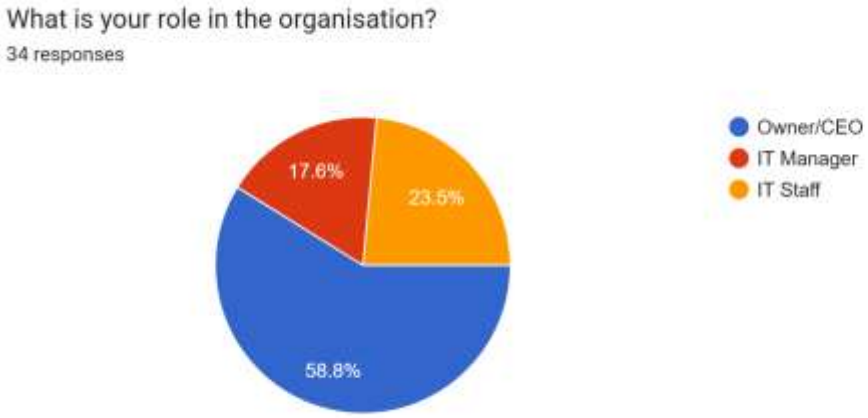
Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 4 | April 2025 -Peer-Reviewed Journal



The survey data reveals the following distribution of company sizes among the respondents:

- **Micro-sized businesses (1-9 employees)** constitute the largest group, with **15** out of the 34 respondents.
- **Small-sized businesses (10-49 employees)** represent the second-largest segment, with **14** respondents.
- **Medium-sized businesses (50-249 employees)** are the smallest group among the respondents, with **5** companies.

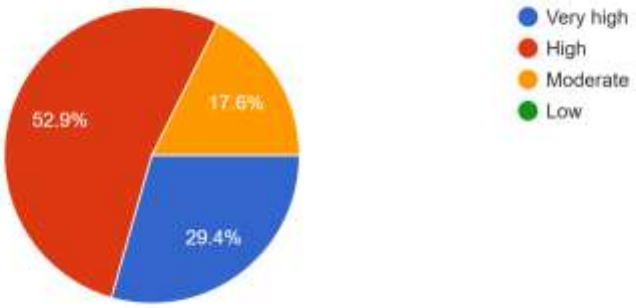
In total, **34** companies participated in this part of the survey regarding their size. The majority of the respondents are from micro and small-sized enterprises, with medium-sized businesses making up a smaller portion of the sample.



Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 4 | April 2025 -Peer-Reviewed Journal

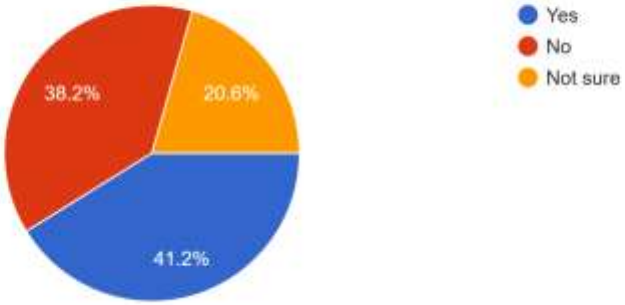
How would you rate your company's overall awareness of cybersecurity threats?

34 responses



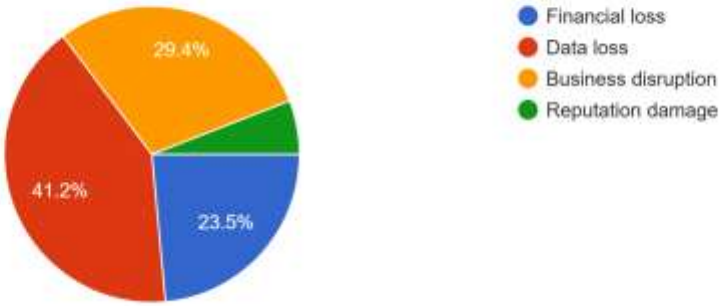
Has your company experienced a cybersecurity incident in the past 3 years?

34 responses



What was the impact of the cybersecurity incident(s)?

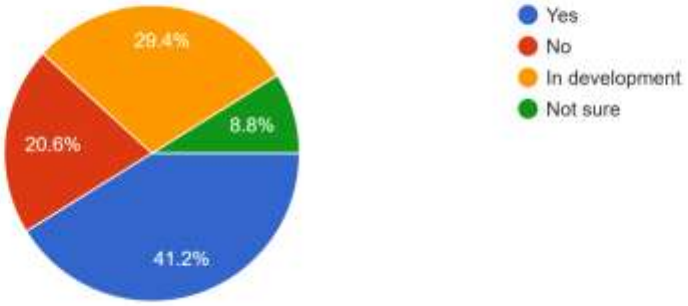
34 responses



Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 4 | April 2025 -Peer-Reviewed Journal

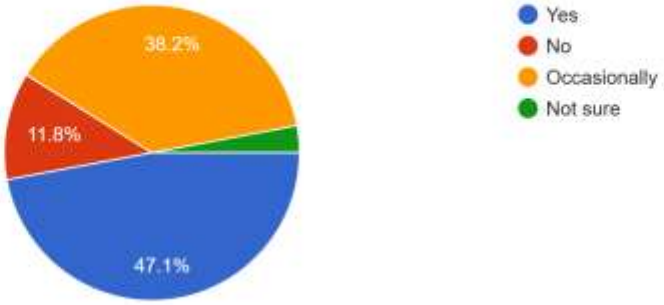
Does your company have a dedicated cybersecurity policy?

34 responses



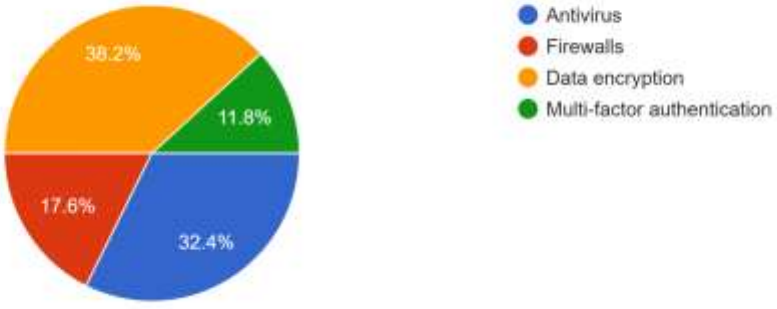
Do you conduct regular risk assessments for cybersecurity threats?

34 responses



What cybersecurity measures does your company currently use?

34 responses



Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 4 | April 2025 -Peer-Reviewed Journal

CONCLUSION

In conclusion, our investigation into the cybersecurity landscape of Small and Medium-sized Enterprises reveals a critical juncture. While awareness of cyber threats exists at a moderate level, a significant proportion of SMEs have already experienced detrimental cybersecurity incidents, resulting in financial losses, data compromise, and operational disruptions. The adoption of fundamental security measures like antivirus and firewalls is common, but the implementation of more sophisticated protections remains limited.

The core challenges hindering effective cybersecurity in SMEs are multifaceted and interconnected. Financial constraints restrict investment in robust security solutions and dedicated expertise. A lack of specialized IT staff further exacerbates the difficulty in implementing and managing complex security measures. Critically, low cybersecurity awareness among employees creates significant vulnerabilities to social engineering attacks. Compounding these internal challenges is the constantly evolving and increasingly sophisticated nature of cyber threats, making it difficult for resource-constrained SMEs to keep pace.

Ultimately, our findings underscore the urgent need for tailored and accessible cybersecurity solutions and strategies for SMEs. Addressing the identified challenges – particularly financial limitations, staffing gaps, and awareness deficits – is crucial for building cyber resilience within this vital sector of the economy. Future efforts should focus on providing cost-effective tools, user-friendly training programs, and clear, actionable guidance that empowers SMEs to navigate the complex threat landscape and safeguard their digital assets effectively.

REFERENCES

1. *CISA (Cybersecurity and Infrastructure Security Agency) – (www.cisa.gov)*
2. *Cyber.gov.au (Australian Cyber Security Centre) – (www.cyber.gov.au)*
3. *FCC (Federal Communications Commission) – (www.fcc.gov)*
4. *NIST (National Institute of Standards and Technology) – (www.nist.gov)*
5. *SBA (U.S. Small Business Administration) – (www.sba.gov)*