Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 15, Issue. 1, January 2026, pg.119 – 136

A Strategic Review of Cybersecurity Threats and Mitigation Strategies in Small and Medium-Sized Enterprises which Focus on Ransomware and Data Breach Risks

Thalabattula Raj Shekhar; Nyabilli Gulshan Kumar

Computer Science, Gitam Deemed to be University, Vishakapatnam, India

DOI: https://doi.org/10.47760/ijcsmc.2026.v15i01.009

Abstract: The current study focuses on the impact of cyberattacks, specifically ransomware, and data breaches on small and medium enterprises (SMEs) owing to their increasing prevalence, as well as cyberattacks in general. Defining the role of SMEs in the global economy as extremely critical, and taking into account the fact that they are financially unstable and lack the technical know-how required to tackle contemporary cyberattacks, the study looks into the lack of cyber awareness as a principal obstacle along with the over-reliance on third parties, and the lack of adequate protective systems. Framing the study around qualitative secondary data and thematic analysis, the study aims to identify patterns in the vulnerabilities of an SMEs - cycle, and assess the mitigation of the patterns through a range of methods including employee training, obtaining cyber insurance, and the adoption of technologies. The findings indicate the pressing necessity to allocate additional funds, to utilize and implement technological systems, to improve the systems of growth, and to implement the adaptive systems as means for cyber resilience. The study aims to cyber risks.

Keywords: cybersecurity, SMEs, ransomware, data breaches, cyber risk, mitigation strategies

Chapter 1: Introduction

1.1 Research Background

Small and medium-sized enterprises represent a vital segment of the global economic framework, contributing significantly to employment creation, innovation, and regional development. SMEs have become even more dependent on interconnected systems for operational efficiency with the increasing integration of digital technologies into business processes and customer engagements. However, the operational efficiency has increased cyber vulnerability for these businesses too.

SMEs are more susceptible to under-resourced cyber security systems than larger businesses. As a result, these businesses pose a low risk with high rewards cyber security systems for malicious actors. Ransomware, breached data, and lost income are the more common cyber abuse. The collapse of services and disruption of trust between the business and the clients further compounds the lost income. There is a lack of basic resources to prepare a defense against these cyber abuses and the lack of basic resources will amplify the negative economic and social impacts.

1.2 Scope of the Research

This research examines cybersecurity challenges faced by small and medium enterprises (SMEs) particularly focusing on ransomware attacks and data breaches. The research seeks to offer scalable approaches that take into consideration the capabilities of small businesses, and consider the current mitigations of security incidents as new technologies like artificial intelligence (AI) and machine learning arise to enhance the capacity to detect and respond to cyber threats. This study also considers the international cyber resilience of SMEs in order to formulate suggestions - practical recommendations for the SMEs themselves, decision-makers, and cybersecurity practitioners - based on best practices and case studies of SMEs that have information to share.

1.3 Aims and Objectives

The main purpose of the paper is to examine cybersecurity threats to SMEs and provide recommendations on the implications of both ransomware and data breaches. The objectives include:

- Identifying and analyzing current practices (including technical ICT cybersecurity resources and the human resources component) to assess achievements.
- Identifying and analyzing existing practices, including cybersecurity technical resources as well as human resource components, to determine the outcomes attained.
- Evaluating consequences of using new technologies such as AI technologies, for improving systems to predict vulnerabilities and threats.
- Describing sufficient and affordable implementation of improvement options in consideration of the capabilities and limitations of SMEs with respect to funds and resources.

1.4 Research Questions

This study seeks to address the following questions:

- Which cybersecurity risks have the most negative impact on SMEs, and in what ways do ransomware and data breaches intersect and impact • What are the current mitigation in place, what are the inhibiting factors and what are the mitigation in place, what are the inhibiting factors and how effective are those factors?
- Within what parameters can the fields of Artificial Intelligence and Machine Learning be utilized to enhance the control of cyber threats in SMEs, specifically focusing on improving the triad of detection, prevention and response?
- • What joint actions can be proposed to improve the cybersecurity practices of small and medium enterprises (SMEs) along with the public and private partners?

1.5 Problem Statement

Considering their significance in the economy, small and medium-sized enterprises will remain at greater risk of being successfully attacked by cyber criminals because they have not invested in defensive technologies and do not have access to deep cybersecurity expertise. The increasing availability of ransomware, and also data breaches in

SMEs, is also indicative of a more broad absence of organized cybersecurity readiness, especially with a lot of SMEs. In contrast with larger corporations, which deploy comprehensive and robust cybersecurity frameworks, small businesses often have far less cybersecurity implemented, which results in a greater likelihood of an inevitable disruption of operations and costly litigation. The discrepancy between the level of cybersecurity, specifically the vulnerability of SMEs, and the lack of available resources raises a need and urgency for effective, inexpensive and adaptable defensive techniques as a result of frameworks.

1.6 Research Rationale

This study has been motivated by an uptick in the incidence and seriousness of cyberattacks against SMEs. Furthermore, there is growing Demand of cybersecurity for businesses to have cybersecurity. SMEs are foundation of the economy both nationally and globally. The vulnerability of these SMEs exposes not only the individual enterprises, but their entire supply chains and the economy, to substantial risk. Most existing research focuses and prioritizes large enterprises, leaving SMEs largely unrepresented in the majority of cybersecurity studies. The purpose of this research is geared at responding to the imbalance by creating and proposing relevant, innovative, and empirical strategies to strengthen the digital resilience of SMEs.

1.7 Structure of the Dissertation

This thesis aims to provide a complete overview of the cybersecurity challenges and the available mitigation strategies for small and medium sized enterprises.

Chapter 1: Introduction – This introduces the Chapter 1 Introduction presents the background of the study, target scope, aims and objectives of the study, research questions to be answered in the study, the problem statement, the rationale for the study, and a summary of the entire dissertation in a logical way.

Chapter 2: Literature Review. Examines and evaluates the secondary data or the existing literature on the cybersecurity challenges within the scope of SMEs, particularly on the challenges posed by ransomware, data breaches or intrusions and analyze the recommendations solutions to address the challenges.

Chapter 3 Methodology outlines the research design, and discusses and explains the method/s of data collection and data analysis that are incorporated to form the study.

Chapter 4: Findings and Analysis – Presents the findings of the study and the case studies, and the statistical outcomes and thematic analysis of SME cybersecurity.

Chapter 5: Discussion – Discusses the findings of the study in the larger context of the research and its significance for SMEs and the stakeholdersa such as decision makers and practitioners in the industry as well.

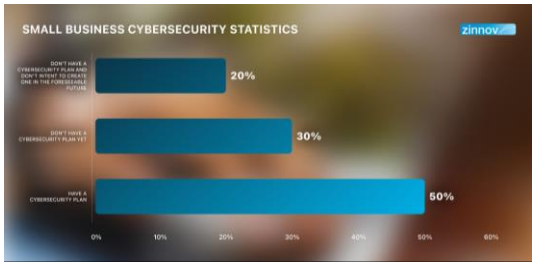
Chapter 6: Conclusion and Recommendations: The last chapter summarizes the findings of the research and proposes actionable recommendations to improve the cyber security for SMEs and identifies the future areas for the cyber security.

Chapter 2: Literature Review

2.1 Introduction

While Small and Medium Enterprises (SMEs) are important to the economy as a source of employment, product innovation, and productivity for the economy, their adoption of digital technologies and online systems to facilitate enterprise processes has drawn them into the dangers of the digital economy. These dangers are compounded due to the limited financial, technological, and strategic resources of SMEs. Because of the interaction of digital technologies and limited resources, there is a significantly higher degree of vulnerability to ransomware incidents. The negative impacts of these threats include interruptions to business operations, substantial financial and reputational losses, and, in the worst case scenarios, total business failure. This chapter will identify the threats of ransomware attacks and data breaches on SMEs. This chapter further unites the extra contributions, and states that primary contributions are also one dimensional, there is no primary focus on the cyber risks, and the cyber security for SMEs is very unprotected.

2.2 Cybersecurity Threats Facing SMEs



(Source: Zinnov 2024)

2.2.1 Ransomware Attacks

Ransomware attacks are one of the most common and complex type of cyber incident impacting SMEs across many situations. In a ransomware incident, an attacker encrypts critical business data and demands that a ransom is paid in order for the organization to decrypt that data, frequently threatening to expose sensitive data to the world. This process of double extortion places an additional layer of pressure onto SMEs, as they often have fewer resources available to manage an incident. The financial implications of a ransomware incident can extend beyond the ransom demand; these may include downtime, loss of data, enforcement action if a breach of regulations occur, in addition to loss of trust from customers. Human error is still a vulnerable weakness that leads to ransomware incidents. Many employees are not familiar with the training that is required to recognize phishing attempts and other activities via email - thus, attackers will be able to use all different types of manipulation in order to take advantage of an organization. Weak password policies as well as ineffective filters in your email systems also place the organization at risk. All of this creates not only an unstable financial environment for the SMEs but also diminishes the credibility of the SMEs in that market, ultimately making it very difficult to keep your customers. Louder implications suggest that there is some type of requirement to organize an integrated process that also uses any type of organizational policy and training for employee awareness programs with technology interventions.

(Source: Monteiro 2024)

2.2.2 Data Breaches

Data breaches pose serious risks to SMEs, resulting in legal penalties, regulatory fines, and long-term reputational harm. To small mediums enterprises, the most typical form of risk in data breaches arise from factors such as weak system access controls, outdated software, and poor encryption, plus, the risks for system breaches are also enhanced from service provider systems. Attackers find it particularly easy to exploit SME systems in order to gain access to larger supply chains which, to other larger corporations, can several lost access points to systems.

The internal risk is also high. Employees can also expose highly sensitive and important information when being negligent and careless on the digital keys and devices. When SMEs breach the law, especially with the regulatory frameworks such as the GDPR, they can be sued and additionally affected by other cash out penalties. The loss of trust from customers also makes it a greater risk for SMEs since the data breach reduces the customer's business opportunities which makes it highly important for SMEs to breach the system. Collection of important data is also risked and, internally, SMEs are also highly affected. Pivotal data reduction makes it important to breach internal

resistant systems in order to gather data effectively. This data and other risks being lost emphasize the need to breach innovative internal systems in data loss and compromised systems.

(Source: Fortinet. 2024)

2.2.3 Other Emerging Threats

Besides ransomware and data breaches, SMEs are affected by other cyber risks including phishing, malware and insider threats. Phishing scams manipulate workers into providing either login credentials or revealing sensitive information, creating further security vulnerabilities. Malware, which includes spyware, worms, and trojans disrupt systems and compromise data integrity often with no immediate detection. Insider threats are difficult, whether they are purposeful or unintentional, because of the unique issues posed in the SME environment where there is very broad, easy access to their systems. The more associates that do not have access to the sensitive systems, that means more potential for misuse, unauthorized access and indiscreet behavior that creates challenges. Insider threats continue to evolve needing security architectures with layers of security mechanisms, continuous monitoring of network activity, and improved employee awareness to better position organizations.

2.3 Unique Challenges Faced by SMEs

2.3.1 Financial and Resource Constraints

Most SMEs function on a specific budget that restricts their capability of engaging in a genuine cybersecurity model. If there is limited finance and budget, SMEs can be limited to depending on tech at a certain or advanced human staffing solutions to identify gaps in vulnerable tech. Further, some have legacy applications that are poorly designed and unlikely to respond, especially rapidly, to applicable hyper-modern attack mitigation techniques or scenarios. Legacy systems used in an SME setting that continue to be relied upon would be significant points of risk that simply are not supported by any vendor service. Furthermore, SMEs are limited by funding to get the technology and devices, both simple and complex that would be needed to secure their assets - costs related to intrusion detection systems or advanced gaps in end-point security would be outstanding costs. Options for support, as government subsidies or arrangements for partnerships to paying professionals, would allow SMEs more affordably deploy cybersecurity products bureaucracy and advanced from experts developing programs gradually and would make cybersecurity a more commonplace concern.

(Source: Cyber Defence Magazine 2024)

2.3.2 Lack of Expertise and Awareness

Another important issue is that small and medium-sized enterprises (SMEs) often do not employ specialized IT personnel and instead depend on their entire staff having, at best, some basic, general training and knowledge of cyber security. This, knowledge and training, does create difficulties in recognizing some of the social engineering and phishing scams. Research shows that there is a considerable advancement in protection when employees of SMEs embrace and integrate security measures of a minimal standard, that is, a password policy, device security, and basic threat recognition, and there is a considerable decline in employees falling victim to attacks of this kind.

2.3.3 Dependency on Third-Party Vendors

Outsourcing vendors contributes another facet of cybersecurity risk to SMEs. Outsourcing a service is cost-effective and scalable; however, a vendor breach can compromise the SME's network that employs the vendor. Fewer SMEs have the technical knowledge to confirm their vendors use good security practices. Vendor risk is best managed with a good working knowledge of risk, practices for risk management, written agreements, ongoing monitoring, and use of contracted framework agreements that cover the most important elements of security compliance.

2.3.4 Limited Incident Response Capabilities

Most SMEs do not have a immediate incident response plan and are not prepared for sudden attacks. With very less time to respond and contain incidents occurs when there are no defined incident management plans, leading to longer lasting outages and more cost associated with recovery. Incident management preparedness to mitigate the impact of a cyber attack requires organizations to design and implement the protocols over time, utilizing exercises, simulations, and tabletops to prepare for, and discuss, indents, and possibly even to hire outside consultant support.

2.4 Existing Mitigation Strategies

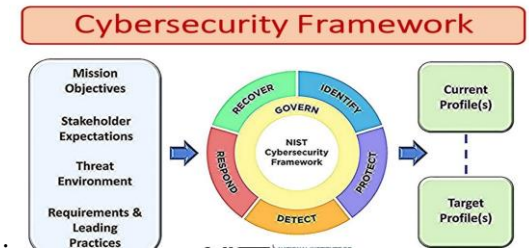
2.4.1 Technological Solutions

Cybersecurity technologies firewalls, encryption tools, endpoint protection systems, as well as active intrusion detection software hold up SME security strategies. A higher level of sophistication in cybersecurity is deemed necessary by some SMEs to supplement the monitoring of their network traffic (and user activity) for irregularities; methods of detection and prevention against unauthorized access; and blocking access to the network entirely.

2.4.2 Cybersecurity Frameworks

Frameworks such as NIST CSF and ISO/IEC 27001 offer structured guidance for risk assessment, control implementation, and compliance management. These frameworks guide SMEs to recognise their weaknesses and put in place ordered security measures.These frameworks face difficulties of having less staff, budget, and advance security

Simplified approaches customised for SMEs could increase adoption and improve overall compliance.



(Source: Feather 2024)

2.4.3 Employee Training and Awareness Programs

A human-centric approach is essential to lowering the risks linked to cybersecurity. Workshops focusing on phishing, on data protection as well as cybersecurity training, mitigate the oversights created by human errors. However, this is not the case for many small and medium-sized enterprises (SMEs), as they do not invest the time, and money in citizen training and hence leave employees unprepared to deal with the adapting techniques in cyber-attacks. Security awareness is therefore recommended to be included as a minimum in the organization's security and compliance framework.

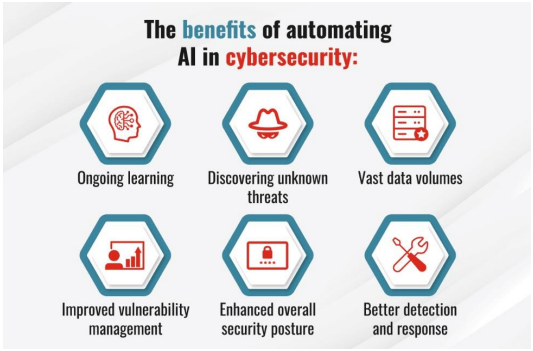
2.4.4 Regulatory Compliance

As business expands the risk of having data breach, misuse of data increases. Compliance requires increased internal control as well as an increased emphasis on risk assessment and mitigation as further regulation may impact the business and or the jurisdiction(s) in which the business operates. For an SME, the ability to develop privacy innovations and adapt to regulation flexibly strengthens their privacy compliance.

2.5 Emerging Solutions and Innovations

2.5.1 Artificial Intelligence and Machine Learning

AI and ML technologies are shaping the future of cybersecurity. They can manage real time detection of threats and can support automated actions to avoid attacks. These technologies allow for the processing of large datasets in identifying anomalies and potential threats giving SMEs a level of protection which was previously accessible only for large companies (Ambreen et al., 2023). At this time, AI-powered solutions are only limitedly available to SMEs because of their expense and the lack of awareness of their capabilities.



(Source: Fortinet 2024)

2.5.2 Cybersecurity Insurance

Almost every businesses and in every industry in the world have been affected financially or operationally because of cyber events such as ransomware attacks and data breaches over the past ten years. As a result, cyber incident financial protection policies have come out and became aware, mainly for Small and Medium Enterprises (SMEs). These protection policies reimburse the affected companies for data recognition and recovery, legal actions, data

breaches and other cyber event related fines, and for loss of indefinite income due to the cyberattack. Insurance policies can protect companies with minimal resources by providing an extra safety net.

However, most of the SMEs do not take these policies because of their high cost of premiums and lack of knowledge. Many companies struggle to articulate complex insurance terminology explaining these protection policies which disinvests them from protection. Simplified insurance policies and heightened awareness could allow for wider adoption of cyber-incident protection policies to SMEs.

2.5.3 Public-Private Partnerships

Cybersecurity ecosystem is collaboration between government entities, industry stakeholders, SMEs. Public-private partnerships and subsidised training schemes are valuable initiatives to support SMEs' awareness through further awareness campaigns (Mutalib et al., 2021). Numerous regional initiatives, such as those targeting SMEs in Wales and Kenya, show a more refined approach towards the needs of a region.

2.6 Gaps in the Literature

There is an extensive body of work on cybersecurity issues affecting SMEs and the protective means to mitigate the challenges, yet numerous topics remain insufficiently studied. Most of the research to date discusses the general cybersecurity phenomenon and has yet to examine specific issues such as the operational challenges related to the resource constrains of SMEs.

In addition to the above, there is a lack of attention to some of the variables related to specific regions, the changes in technology, and the human factors that influence the outcome of such problems. These observations reflect the need to continue studying these issues/deficiencies, which, frame work is more applicable and flexible to small and medium enterprises.

2.6.1 Awareness of SME issues:

Much of the research in cybersecurity is still focused on large organisations with little consideration of the unique situations that SMEs find themselves. SMEs are often operating on low budgets, lacking technical experience and systems to use more advance security infrastructures. Even so, many studies do not take this into account.

As there is little research representation, generic cybersecurity recommendations are less beneficial to SMEs. Therefore, these small businesses are developing security practices based on what larger organisations are conducting, instead of reflecting their operational capacities.

2.6.2 Lack of Attention on local and industrial SMEs:

There is an absence of focus disruption of day-to-day services caused by small and medium enterprises (SMEs) within the geographical areas of varying regulatory frameworks. Differences between regional frameworks, optences, and cybercrime threats are largely ignored by the literature.

Healthcare, retail, or finance are in particular sectors that may be under consideration. Lack of in-depth analysis and research specific to these sectors impacts the research and the recommended mitigation strategies that follow the analysis of the evidence.

2.6.3 Gaps in the Cybersecurity Awareness:

Human behaviour continues to be one of the largest vulnerabilities of SMEs concerning cybersecurity, and it is largely unexplored within the research literature. Although several studies illustrate the value of training and awareness initiatives for staff, little focus on how these may be adapted to fit the operational realities of SMEs Addressed the reported phenomena's scarcity or absence regarding awareness models that are affordable and scalable despite the struggles of SMEs over the cost and resource availability such as time and human capital. Also, there are neglect of the psychological variables motivating the employees' adherence and disobedience to the compliance of the cybersecurity protocols such as their inclination toward the cyber issues, managerial values, and uneasiness toward the cyber awareness. Ineffective disregard on cultivating a 'band' mentality or culture on cybersecurity awareness in the context of the small firm, results in employees displaying the behaviours of. The stakeholders are more prone to phishing, social engineering, and data breaches as a result of a lack of awareness and cybersecurity practices.

The expression of focused behaviours more reflective of an SME's working environment should inform research on behaviours that promote awareness or are measurable for low resourced firms.

2.6.4 New Cyber Risks and Technology innovations

Current literature mostly focuses on traditional dangers like phishing and ransomware attacks while ignoring new types of digital threats. In particular, most literature has not studied the context of small and medium enterprises (SMEs) concerning new types of cybercrime including attacks driven by artificial intelligence, deepfake technology, manipulation, and other risks associated with quantum computing. Within the context of the SME sector, these types of advanced technology risks are especially concerning because SMEs often lack the technological infrastructure and human capital required to mitigate the most advanced forms of cybercrime.

Moreover, while the larger cybersecurity ecosystem understands the potential of artificial intelligence (AI) and machine learning to mitigate threats, there is a lack of empirical evidence which is SME-centered on the low-cost implementation of these tools. Few empirical studies examine the high degree of practical constraints (including cost, technical restrictions, challenges SMEs face when trying to implement cutting-edge cybersecurity tools) and how this contributes to SMEs the inability to use technological advances in cybercrime as a form of innovation. In other words, cyber innovation. failure to innovate.

2.6.5 Lack of Long Term Research

Most existing studies of SME cybersecurity are cross-sectional and offer only short-term views of challenges and the responses to them. This results in an incomplete understanding of how SMEs change and adapt to their security practices over a longer duration. Given the flexible nature of cyber threats, longitudinal studies are required to assess the degree of effectiveness in risk management initiatives over a prolonged duration.

Longitudinal studies would inform us about how SMEs respond to emerging threats, how long the solutions endure, and how resilience evolves over time. This study would also help decision-makers and policymakers identify the most effective long-term digital security solutions.

2.6.6 Limited Research on Cyber Insurance

sed on what studies have shown, most have addressed the benefits of purchasing cybersecurity insurance for risk management, however not enough justification has been made to the rationality of why this coverage, specifically, would improve the average SME cybersecurity posture. In most studies, coverage has been shown to improve posture through reduction of access. The average gap in understanding has most likely been attributed to the following reasons: the complexity of the policies, the policies being tailored to the enterprise rather than the SME, high premiums, the policies being designed with coverage to access rather than access to coverage, and the policies being lefone of with little to no coverage, paralysis, and or indecision to move the positive premiums.

The cybersecurity insurance market is a small fraction of overall insurance coverage. The SME market for cybersecurity is shrinking at a continuous exponential rate, and the overall SME market is in a similar state. The market being as closed as it is, it offers little to no evidence for SME participation.

2.6.7 Insufficient Cooperation Between Stakeholders

The cybersecurity insurance market is unstructured and highly uncoordinated. As is the evidence at hand. There is minimal public and private partnerships established in this domain of unstructured and uncoordinated evidence. The absence of redundant inter-temporal multi functional cooperation planned for in the unstructured SME device market runs the SME market to a lack of evidence, specifically to an unstructured cybersecurity device market. The absence of innovative evidence in parallel with a no zone of evidence runs the EU to limit constructive critiques based on unencumbered evidence, which the security of the SME market relies on.

The absence of inter functional public and private partnerships based on uncoordinated evidence has resulted in unequipped SMEs.

2.6.8 Challenges from Security Practice

Numerous scholarly debates continue to exist on an abstract level, having almost no practical value when it comes to the ways in which SMEs might incorporate the daily use of cybersecurity strategies into their routines. SMEs often tend to struggle the the balancing of the cybersecurity spendings and the essential operational expenditures which leads to a an inconsistent protective measures adoption or sometimes even a very low degree of adoption.

In addition to this, descriptions of lower-cost security measures tend to be absent from available literature. This leaves SMEs with no clear recommendations to follow in order to secure their systems and to establish a more cohesive approach to their actions and to reduce their security exposure. This can be taken as a clear invitation for studies that could offer concrete implications for practice where the purpose is to inform what strategies might be adopted in settings with clear resource constraints.

2.7 Conclusion

The chapter has reviewed all relevant literature on cybersecurity risks and the available defensive mechanisms on ransomware and data breaches for Small and Medium Enterprises (SMEs).

It elaborated on the systemic weaknesses regarding the interplay between the organisational structure, the technological capabilities, human behaviour and constraints with policy formation.

These reviews points to a need to practitioner in searching for, developing and improving applicable, scalable, and contextualbased solutions that connect to the reality of operational conditions facing the SMEs. Future research should seek sustainable security practices with customized strategies per location and topic. This serves as a basis for the project's following chapters in order to share recommendations to improve overall cyber-resilience.

Chapter 3: Research Methodology

3.1 Introduction

Research Methodology This chapter describes the Research Method used to address the objectives and questions posed in this research. The reason for collecting of secondary qualitative data and the thematic analysis as the main methodology is also explained in this chapter, along with the importance of qualitative data in understanding cybersecurity threats, mitigative strategies and the unique challenges faced by SMEs. The study both combines useful insights from reports, case studies and existing research. In qualitative approach, this method is selected because it studies the subtle experiences and vulnerability of the SMEs since it provides profound understanding of the phenomenon.

3.2 Research Design

In this study, a qualitative descriptive method has been adopted based on data collected from thematic analysis, based on secondary. The definition of Qualitative research is appropriate for resolving research problems focused at resolving the complexity and heterogeneous nature of the cyber threats faced by the SMEs. Unlike the more technical forms of Quantitative research involving graphs and numbers, Qualitative research offers deeper access to the enterprise and the individuals` experiences. Throught this way, the casual mechanisms leading to the identification of vulnerability of the SMEs can be identified, and the effectiveness and efficiency of current mitigation strategy can be understood, also identifying alternative measures. For this purpose we chose secondary data collection from existing studies, industry reports, case studies and governmental material, as they were relevant to cybersecurity subject matter and also valuable sources of data.

3.3 Secondary Data Collection

Secondary sources are indeed justified in this work. Secondary data involves a data synthesis as opposed to collecting new data Secondary data collection was preferred here as there was solid and credible material on SMEs and cyber security including scholarly works, industry analyses, government documents and commentaries by recognized authorities. The secondary data gave information on regions where cyber security was breached and ransomware attacks on SMEs and the steps taken to secure data.

Secondary data is the ability given to authors to use existing work, and this permitted the authors to have a comprehensive view of the risks cyber security posed to SMEs without the hassle of collecting primary data. The secondary source authors had a virtually unlimited capacity to engage in multi-faceted analyses, which certainly increased the authenticity and reliability of the results. Similarly, the secondary sources systematically tackled the questions on cyber security in SMEs and the interplay of three components which were technological, organizational, and human factors.

3.4 Thematic Analysis

Thematic analysis was chosen as the principal qualitative method for analyzing the dataset of secondary data because it can be used to recognize and identify important patterns across data sources and to provide an interpretation of these patterns in the appropriate context. Thematic analysis is applied through thoroughly reviewing the dataset, developing an initial set of codes, then generating larger themes that respond to the research aims of the study.

Through this organised process, the study was able to develop meaningful themes from complex data, highlighting critical discussion topics such as: challenges in cybersecurity, weakness in an organisation, and prominent mitigation strategies. Thematic analysis gave sufficient flexibility in ensuring pre-existing trends and emerging new trends were captured effectively.

3.5 Rationale for Methodology

The research design used in this research closely matches the intentions of the study and mirrored the complicated nature of the cybersecurity problems faced by SMEs. The decision to use only secondary data was finally taken since secondary data allows for broader scale analyses of various forms of evidence from various academic and industry-based sources, thus increasing the breadth and depth of understanding of the complexity that is being considered.

Thematic analysis was appropriate because it is built to advance pertinent themes associated with repeating patterns in the qualitative data, to identify, classify and summarize themes that emerged from the study with respect to the three pillars of cybersecurity (technological, organisational and behavioural). The literature review methods for secondary data gathering and the thematic analysis were suitable to examine the complexity of the vulnerabilities and resilience mechanisms inherent in security practices experienced by SMEs.

3.6 Limitations of the Methodology

Notwithstanding the advantages of the chosen methodology, there is always going to be some possible intrinsic limitations. For example, the limitations of the secondary data mean that the analysis is confined to pre-existing data that may not capture the true extent of the multiplicity of the phenomena that SMEs face at different geographical locations. Inconsistencies in prior research\, especially the coverage and quality of the research, will always play a role in the variation of the multiple findings of the present research.

Thematic analysis also suffers from some interpretation bias, a problem that results from the oversight of the researcher in the selection and allocation of the several themes. Even though a lot was done in a bid to try and safeguard objectivity, forms of bias that result from people's choices are not possible to completely eliminate. Some of the limitations for not being able to collect primary data might include the access to and engagement with the stakeholders of the SMEs, and the timely collection of primary data, which would enhance the richness of insights from practical knowledge. The predictions of other research might improve the reliability and accuracy of the research outcomes with data that are a combination of both qualitative and quantitative research.

3.7 Ethical Considerations

This study upheld ethical responsibility by relying entirely on information obtained from publicly available and previously published, pre-existing sources. All cited materials were evaluated for credibility and relevance, and all referenced items evidenced proper citations of the original authors.

This study did not create or misrepresent evidence and sought to yield an accurate and impartial account of the literature available. This approach to ethics ensured that the research remained true to ethical standards of academia and described a transparent approach to all evidence analyzed.

3.8 Conclusion

This chapter discusses the methodology applied during the research focusing on secondary qualitative data gathering and thematic analysis. It therefore aims to develop a deeper understanding of possible cyberattacks and their preventive measures as well as the distinctive issues associated with SMEs by synthesizing the findings from the

research, reports, used in case study. In analysing the data the thematic framework in data guarantees that observations are orderly and well-organized; thus, the findings are based on evidence and are relevant to the goals of the research. Despite its limitations, the approach has provided a platform to address a research question and meet objectives. The knowledge acquired from this will be the foundation of the chapters focusing on results, discussion and recommendation.

Chapter 4: Analysis and Results

4.1 Introduction

In this chapter we discuss the information gathered from various secondhand sources regarding important cybersecurity challenges for SMEs. The discussion describes how ransomware attacks and data breaches interrupt business operations and leak company's sensitive data.Through the examination of patterns across a number of studies, this section lays the groundwork for the identification of the main themes that characterize SME cybersecurity vulnerabilities and how effective mitigation strategies are currently in place.

4.2 Insights from the analysis

The Research analysis summarizes four areas that can build current cybersecurity systems effecting SMEs. The areas are increasing cyber threats, structure of SMEs which operation network , performance of security measures and adapting latest technologies for better solutions. Overcoming these areas of cyber threats and attacks provide bigger view of understanding how SMEs are affected by everyday increasing cyber attacks and their risks

Each area represents a unique problem but still they are interconnected in cybersecurity network. The growing advancement of cyber attacks shows how attackers are adapting their latest technologies to easily threat SMEs. At the same time SMEs struggle with resources and skills, which restricts SMEs from responding effectively. The analysis shows that while current strategies prevent protection to some level but they are not effective for long term and complex threats.

4.3 Continuously Growing cyber threats:

In this section, we will investigate the pervasive and ongoing cybersecurity threats to small to medium enterprises (SMEs), indicating how these threats have become increasingly prevalent in everyday digital business operations. As more business activity moves into the digital environment, and increasingly revolves around online transactions and interdependence, exposure to cyber risk will invariably increase, and the risk of catastrophic failure for SMEs due to malicious behaviours will be higher.

A key factor of this spreading threat attacks can be seen because of increasing of ransomware and data breaches. These attacks usually target SME because they have comparatively weaker security than Big industries. When planning these attacks criminals see SME as their easier targets since SMEs can not detect advance level threats. Hence even smaller problems can give access and invade networks

Research shows that these cybersecurity attacks do not only exploit their financial systems but also gain access and mis use dimensions of SMEs such as enterprise data, customer data, service data. When cyber attacks happen many SMEs shut down which causes missed business opportunities and loss of customers. In some situations , the cost of recovering is greater than what organization has lost and may eventually shut down the business.

Another important observation regarding the improving nature of cyber attacks. Attack techniques are being more advanced over the time. Cyber criminals these days are using techniques like automated malware, phishing, social engineering. These methods use humans weakness to manipulate employees and use them as entry point for attacking.

Actions like remote work, internet related technologies cause cyber security problems .These technologies can also help minimizing cyber attacks but also can lead to them SMEs may have a difficult time achieving sufficient protection for operations securely, often providing uneven coverage for different operations, which will pose a greater risk of cyber threat engagement.

In addition, a lack of organized cybersecurity governance can influence the prevalence of such threats. Many SMEs lack dedicated cybersecurity personnel or structured risk management strategies and this limits their capability to

respond in a timely nature to an event. Without continuous monitoring and proactive strategies in place, threats could be undetectable until the company had sustained significant damage.

Overall, findings affirm that an embedded nature of cybersecurity threat exists in SME digital ecosystems and necessitates inclusive, ongoing, and adaptive security strategies. Dealing with the embedded nature of threat requires us to move away from reactive responses, to proactive prevention, alongside staff awareness and policy enforcement and in the context of sustainable investment in cybersecurity infrastructure.

4.4 Multiple Barriers confronting SMEs

The second of the major themes that featured concerns the different types of challenges managing cybersecurity threats. Financial and resource constraints appear first. Most SMEs are operating with limited resources and, where needs for day-to-day operations take precedence over investing in cybersecurity infrastructure, this makes it difficult for them to invest in more advanced tools, specialised technology professionals conduct regular security assessments. Vulnerability is also increased in situations where older technologies or better solutions are used.

Another challenge is the lack of experience and knowledge. Even those assessments also showed that most employees and managers in the SMEs do not have enough information on how to handle cyber threats and best practices; leaving them prone to phishing and social engineering. According to Adriko and Nurse, 2024, and what discourages the SMEs to develop a strong culture of awareness and resilience. Also noted are poorly designed training programs and a lack of commitment from Organisational level.

That is another disadvantage as SMEs depend mostly on third-party suppliers. Although third-party services can often be cheaper and are more easily scalable, there are still risks due to potential breaches of security by third-party vendors. Most SMEs suppose that the vendors they contract have enough security measures in place, but this analysis opposes. This brings us to the security vetting of vendors, and their overall security risk management to lose security risk management. Most SMEs do not have the necessary technical skills and resources to perform checks.

Another disadvantage is that many do not have formal incident response plans. The reality is that most SMEs do not have the ability to respond to cyber incidents, thus increasing recovery time and the overall cost and disruption of the attack. Cyber Resilient Organization report by IBM states 77% of organizations, including SMEs, do not have formalized incident response plans. The bottom line, to put it simply, is that incident response planning can no longer be an afterthought when designing the cybersecurity framework of the SMEs.

4.5 Effectiveness of Existing Mitigation Strategies

The third theme looks at whether present reduction approaches are adequate to shield SMEs from the atck of cybersecurity risk. Many technologies, such as firewalls, intrusion detection systems, and endpoint protection software, have been touted for protection. However, analysis shows that these technologies that are non-adopted and incompetently used. Most depend on simple tools that can no longer defend against present day attacks. Next-generation technologies involving artificial intelligence and machine learning will provide more detection-oriented features and capabilities, but their implementations are still constrained by economic means and complexity of modes of operation.

NIST CSF and ISO/IEC 27001 have been successfully used as very good tools to build the overall security posture in many SMEs. These can help in building risk assessment, incident response, and the satisfaction of regulatory obligations. Yet is not well used due to a lack of resources and know-how on the part of SME. A sweat version of such frameworks, especially built for small organizations, can eliminate all that. The first such interventions have to do with the employees themselves; employee training and awareness is needed to minimize risks introduced by human error. Classes teaching employees how to recognize phony emails or messages, how to protect sensitive information, and better understand compliance with the wide range of cybersecurity laws and regulations reduce an enterprise's exposure. An analysis of findings suggests, however, that most small and medium enterprises underestimate this practice and expose their workforce which is generally incapable of combating today's cyber threats. The second is regulatory compliance such as GDPR data protection. It does improve security, but the cost and extra admin work are difficult for SMEs, especially because they do not have sufficient resources.

4.6 Transformative Potential of Emerging Solutions

The fourth theme relates to the potential of innovation in solutions to support SMEs effectively than before in regard to building resilience in cybersecurity. With AI and ML tools with real-time threat detection capabilities detecting abnormal and harmful threats, and responding automatically, and advanced analytics in the ability to process large volumes of data, in regard to security SMEs now have capabilities previously accessible only for larger organisations. However the study found that the adoption is shortened cost and a lack of understanding of AI tools.

Promising a solution to reducing financial risk from cyberattacks is cybersecurity insurance. These policies provide cover in both financial terms and promote observance of a culture of best cybersecurity practice such as regular auditing and compliance of standards for security. In a resource constrained environment insurance helps address gaps in the SME's security posture, and in such situations , as maintained by Adriko and Nurse (2024). However the, barriers to adoption comprised complexity of the insurance terms as well as an absence of information about its benefits.

Involvement of governments, industry bodies and SMEs underpins resilient cybersecurity ecosystems that are crucial for the global economy. Initiatives implemented to support SMEs comprise subsidized training initiatives, public-private partnership, and awareness programs. Regional examples of SMEs in Wales and Kenya show highlight a shift towards a localization approaches to move beyond the challenges experienced there. This suggests that cooperation of stakeholders should be encouraged in designing such programming, and the long-term success.

4.7 Discussion of Key Findings

The research shows that SMEs experience cyberattacks because their digital infrastructures, strategies, and employee usage of digital workplace civility are all lacking sufficient attention in safeguarding their business. As cyberattacks increase in number, SMEs need to understand that while tech tools reduce some risks, they are insufficient all about. It is not that there is a need for better staff training. It's more about accountability and attention to detail that staff need to take to mitigate their careless actions that often open the digital gate to intruders. More than a few SMEs have cybersecurity tools, but the tools and employee training gaps work together to create a situation of 'do the best we can with limited resources, and limited training.'

Stronger, more user-friendly innovations are available, such as cyber insurance, AI systems for fraud and intrusion protection, and inter-organizational partnerships. More SMEs, however, still require simpler, more cost-effective, and more seamless integrations of cyber security processes for day-to-day business. When businesses have to continually work with frictionless systems that intergrate to their day-to-day activities, they can better their business activities with more assurance, thereby likely maintaining better security.

4.8 Conclusion

The serious gaps related to SME cyber security being prepared is further reinforced by the overall results. Windfall to their resources, SMEs remain highly vulnerable to ransomware and data breaches, lack of holistic security strategy, and ineffective adoption of existing industry frameworks to improve. This section summarises the repeating themes around the SMEs needs for realistic, economical, and scalable approaches

Chapter 5: Discussion

5.1 Introduction

Frameworks like NIST CSF and ISO/IEC 27001 give SMEs a good basis for establishing and improving the quality of its cybersecurity posture by facilitating formal risk assessments, incident response and compliance. Inspite of that disadvantages , are that they could not invest more money and lack advance security. Simplified versions or SME-specific frameworks could dramatically reduce barriers to utilization and encourage wider use by small organizations.

5.2 Cybersecurity Threats Facing SMEs

Though the chief aim of the study aims to identify critical issues in the field of cyber security in the small and medium engrossing enterprises (SMEs), the study's results propose ransomware and data breach issues, along with

the cyber security issues, data breaches and ransomware, to pose the greatest risk among other threats. Over time, cyber threats ranging from ransomware with Sophisticated high-level encryption with double extortion or economic ransom to other ransomware that leaves victims with the loss of substantial funds or even loss of reputation or substantial funds, have posed threats to SMEs. There are enormous issues to enterprises to the extent of suffocating the enterprises from their potential ability to manage the distribution of their resources in the enterprises cyber extortion of threats where the threats of releasing the data or even personal files of an enterprise are kept in ransom.

The SMEs are also the source of their own data breaches. Hence, from their data breaches, SMEs have the inability to control and is the source to the architectural, infrastructure phenomena. The phenomena include isolates of control access, control access in high system to Gate Control Weak, system to other vendors third parties. SMEs have been breaches are leaves, and serves as bottom points to geared focus of threats. Phishing, malware threats, and breaches threats from insiders, as well as other threats, also manifest and are interwoven as a whole to multiply the effects of the undetected or even the not been managed breach. The response to the phenomena demands the SMEs to control and mitigate their internal focal points from the external engagements and threats with a defensive strategy that is, depth of threats, extensiveness of internal and external threats, or multilayered.

5.3 Challenges Faced by SMEs

The problems explained in the study tells the reasons why most small and medium-sized enterprises (SMEs) are not able to have advanced cyber protective practices, main reason is low budget funding , because of this we can not purchase advanced protective systems and hire employees to manage security evaluations.Even more alarming, many SMEs operate outdated equipment or no protection whatsoever.

The second barrier is insufficient knowledge and skills among management and employees; leading to limited capabilities in identifying and responding to cyber intrusions across the whole organization. Furthermore, SMEs tend to allocate critical responsibilities to subcontractors allowing for the opportunity for potential indirect risk. Most critically, barriers exist by not having basic cyber policies, nor an incident response plan, to diminish preparedness.

5.4 Evaluation of Current Mitigation Strategies

Although small and midsize enterprises use different defensive strategies such as firewalls and antivirus as well as basic encryption software, those basic defensive mechanisms are countered by most modern cyber threats. More complex defensive mechanisms are often not used due to cost and lack of technical knowledge.

Practically all companies of this type are aware of the most advanced tools and frameworks, but they still do not implement these quantifiable frameworks. Furthermore, most businesses do not give appropriate regard to employee training, despite the utility of such training. This leads to the lack of a cohesive and sustainable strategy regarding this type of cyber threat.

5.5 Emerging Opportunities for Improvement

As of now, unlike any other technology, Imitative learning systems pose ultra promising advancements for small and medium sized enterprises cybersecurity. It is fostering automated cyber defense systems and providing threat identification in real time. Adoption of these systems encounters severe limitations. There is virtually no awareness from the systems and cyber defense are often high in cost.

Government sponsored cyber defense systems are gaining traction, albeit slowly and at a mediocre pace. Issues of being cybersecure and little knowledge on systems led to being compromised. It is getting even worse for small and medium sized enterprises.

5.6 Addressing Research Questions

The results clearly address the study's research questions. The specific risks to small and medium-sized enterprises (SMEs) are ransomware, data breaches, phishing, malware, and insider threats. Even though SMEs implement mitigation measures, these approaches are only effective to a degree, and are limited due to cost and technical restrictions. There are useful technologies such as artificial intelligence and machine

learning, but SMEs have to minimize cyber attacks by making technologies lesser complex and easily accessible to them.

5.7 Implications for Practice and Policy

Based on the findings, SMEs need to observe the importance of cybersecurity through organized training, greater focus on incident response planning and system update protocols, and shift cybersecurity from the visibility stage to the action stage.Policy makers should help SMEs by making low cost tools and training them. The collaboration of the public and private sectors to facilitate operational public-private partnerships will also strengthen and lessen systemic risks.

5.8 Conclusion

This chapter combined the research related to cybersecurity threats, challenges, strategic responses in SMEs, and analyses the remaining gaps in the field and the need to address the knowledge and financial gaps while fostering concrete, scalable solutions. This knowledge will aid actionable recommendations that will be provided in the next chapter, aimed at building SME cybersecurity resilience.

Chapter 6: Conclusion and Recommendations

6.1 Conclusion

This research considered looking at different challenges surrounding cybersecurity. Small and medium-sized enterprises (SMEs) face cyber challenges specifically concentrating on ransomware attacks and data breaches. The study used thematic analysis on secondary qualitative data to determine the type of vulnerabilities the SMEs have which include financial constraints, limited in-house expertise, dependencies on certain vendors, and most importantly, lack of proper incident response plans.

This type of challenges reduces the cyber resilience of SMEs which is solvable. To illustrate, there are even established mitigation frameworks, not to mention the many available structured technologies. Unfortunately, the positive impacts of the mitigation frameworks are limited due to unexplained technological barriers.

There are many problems that need to be resolved but most people around artificial intelligence (AI) emerging technologies, collaborative cyberdefense for cyber resilience, and even more novel versatile cyber collaborative technologies facilitate cyber defense protection. The need for SMEs to build systems, specifically cyber resilience systems is emphasized in the study to legislators, regulatory body for SMEs, and even industry SMEs.

6.2 Recommendations

Enhancing Financial Support for SMEs

Subsidies and incentives offered by governmental and industry stakeholders can minimize the financial cost in deploying cybersecurity measures. Low-cost access to advanced security and shared service models will enable SMEs to implement protection at a reasonable cost, and build security controls over time.

Raising Understanding and Competence in Cybersecurity:

SME staff should be offered refresher training-and-awareness sessions on a regular basis to reinforce their understanding of cyber risk, and appropriate practices to mitigate risk. This will begin to solidify a positive culture in organizations, and reduce human weaknesses to some extent.

Strengthening Vendor Management Practices:

SMEs must implement strict vendor assessment procedures and establish cybersecurity clauses within contracts to minimise third-party risks.

Developing Incident Response Capabilities:

Public-private partnerships and regional cybersecurity hubs should be promoted to support SMEs with shared expertise and resources.

6.2.1 Enhancing Financial Support for SMEs

The financial side of creating effective cybersecurity for SMEs is the most significant part of the challenge. Security investments have to be made by SMEs given the government’s and industry bodies’ sponsorship and the tax

advantages. Lower cost burdens are brought by the subsidies and tax breaks when new advanced tools are added, periodic audits are conducted, and cybersecurity staff are hired. In addition, the corresponding public-private partnership can reduce the financial burdens by providing SMEs with more sophisticated and costly cybersecurity tools and services. SMEs must collect resources carefully while focusing on the other parts of the business by identifying that cybersecurity is an equally important part of operational self-sustainability by allotting the needed resources to it. This can also support their overall security posture along with reasonable protective measures avoiding financial strain and cost overruns when collaborating with MSPs and vendors that offer advanced tools and cybersecurity services at affordable cost.

6.2.2 Building Cybersecurity Awareness and Expertise

The study has demonstrated the existence of a knowledge gap among SMEs. Every employee and manager should attend full training sessions to understand the cybersecurity risks and practices. Skill such as detecting phishing attempts, proper encryption, other security measures, should be taught in such programs. Such training sessions should improve them for upcoming threats and innovative developments, and should be periodically conducted on a regular basis. The main key participants in such initiatives can be industry stakeholders and policymakers. If training programs are offered to SMEs at zero cost or on reduced cost basis, access to these programs will be easier. Programs that focus on the owners and employees of SMEs will instill these individuals as vigilant and responsible employees of organizational culture.

6.2.3 Strengthening Vendor Management

To help limit engaging in cyber risk, small and medium-sized enterprises (SMEs) must establish stricter evaluation processes when considering and managing third-party vendors. Establishing cybersecurity clauses in contracts will establish accountability and ensure that the vendor is aware of and follows established security protocols.

Having frequent assessments of third-party vendors' security and ongoing monitoring of vendors' practices will reduce indirect risks altogether. Improving vendor risk management will help SMEs contribute to better vendor management of risks that affect a safer online world and reduce the risk of indirect and compromised vulnerabilities from third-party vendors to its business.

6.2.4 Developing Incident Response Capabilities

One of the fundamental vulnerabilities of SMEs is lacking no formal incident response plans. Every organization should develop incident response plans and the protocols designed for dealing with incidents should address identification, containment, and mitigation of cyber incidents, communication with stakeholders, and restoring operations. These plans should be practiced, reviewed, updated on a daily basis to make sure they remain effective. Advisory agencies and industry bodies should develop basic templates and guidance in an incident response planning process to develop exposures for SMEs.

6.2.5 Encouraging Collaboration and Partnerships

A more secure digital environment relies on collective effort from all individuals. Government , industries, tech companies, and businesses all need to work together to help and support SMEs. The desired outcome of this effort will be to help SMEs get things, with easier entry into shared resources. Furthermore, reasonably priced training options must also be made available, or to have more opportunities. And it may ensure increased entree into technology.

6.2.6 Collaborative Promotion of Cybersecurity Initiatives

Building collaborations from small and medium sized enterprises (SMEs), governmental organizations and technology companies is critical for enhancing cyber preparedness. Joined resources, discounted training initiatives and awareness campaigns, which work together to build strong collective defence options.

Such collaborative efforts can enable the sharing of lessons learned, provide technical capacity and jointly access higher tiered security tools, more efficiently, than alone. Informal networks help establish strong networks between stakeholders, and collectively build resilience among SMEs, connected in the practice of becoming more cyber resilient.

References

[1]. Adriko, R. and Nurse, J.R., 2024. Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review. Information & Computer Security, 32(5), pp.691-710.

[2]. Ambreen, L., Jain, M., Yadav, R.K. and Loonkar, S., 2023. Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review. Multidisciplinary Reviews, 6.

[3]. Ansar, N., Parveen, S., Alankar, B. and Khan, I.R., 2024, March. Cost-Effective Cybersecurity Framework for Small and Medium-Sized Enterprises. In International Conference on Deep Learning and Visual Artificial Intelligence (pp. 133-155). Singapore: Springer Nature Singapore.

[4]. Chidukwani, A., Zander, S. and Koutsakis, P., 2022. A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. IEEE Access, 10, pp.85701-85719.

[5]. Mutalib, M.M.A., Zainol, Z. and Halip, M.H.M., 2021, December. Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework. In 2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE) (Vol. 6, pp. 1-6). IEEE.

[6]. Neyole, J., Okwiri, S.M. and Mapema, N., 2024. Exploring the Impact of Cybersecurity Threats on Small and Medium Enterprises' Performance: A Case Study of Kajiado County, Kenya.

[7]. Papathanasiou, A., Liontos, G., Katsouras, A., Liagkou, V. and Glavas, E., 2024. Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era. Journal of Information Security, 16(1), pp.1-43.

[8]. Tam, T., Rao, A. and Hall, J., 2021. The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. Computers & Security, 109, p.102385.

[9]. Truong, T.C. and Nguyen, H.K., 2024, May. Cybersecurity in Small and Medium-Sized Enterprises: A Bibliometric Analysis. In International conference on From Smart City to Smart Factory for Sustainable Future (pp. 392-402). Cham: Springer Nature Switzerland.

[10]. Monteiro, P. (2024). SMEs, cyber threats, and cyber attacks worldwide. LinkedIn Pulse.

[11]. Fortinet. (2024). Data breach. Fortinet Cyber Glossary.

[12]. Cyber Defense Magazine (2024). Top 6 security challenges of SMEs. Cyber Defense Magazine.

[13]. Feather, F. (2024). Cybersecurity Framework: 6 Steps. LinkedIn Pulse.

[14]. Fortinet. (2024). Artificial intelligence in cybersecurity. Fortinet Cyber Glossary.

[15]. Zinnov. (2024). Why SMB cybersecurity is a non-negotiable today. Zinnov Blog.

